Converged Access 및 Unified Access WLC 컨피그레이션의 중앙 웹 인증 예

목차

소개

이 문서에서는 WLC(Converged Access Wireless LAN Controller)에서 그리고 Converged Access WLC와 Unified Access WLC(5760 및 5760과 5508) 간에 중앙 웹 인증을 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco WLC 5508, 5760, 3850에 대한 기본 지식
- ISE(Identity Services Engine)에 대한 기본 지식
- 무선 모빌리티에 대한 기본 지식
- 게스트 앵커링에 대한 기본 지식

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco IOS® XE 릴리스 3.3.3을 실행하는 WLC 5760
- Cisco Aironet OS 릴리스 7.6을 실행하는 WLC 5508
- Cisco IOS XE Release 3.3.3을 실행하는 스위치 3850
- Release 1.2를 실행하는 Cisco ISE

구성

> **참고**: 이 섹션에서 사용된 명령에 대한 자세한 내용을 보려면 Command Lookup Tool(등록된 고객만 해당)을 사용하십시오.

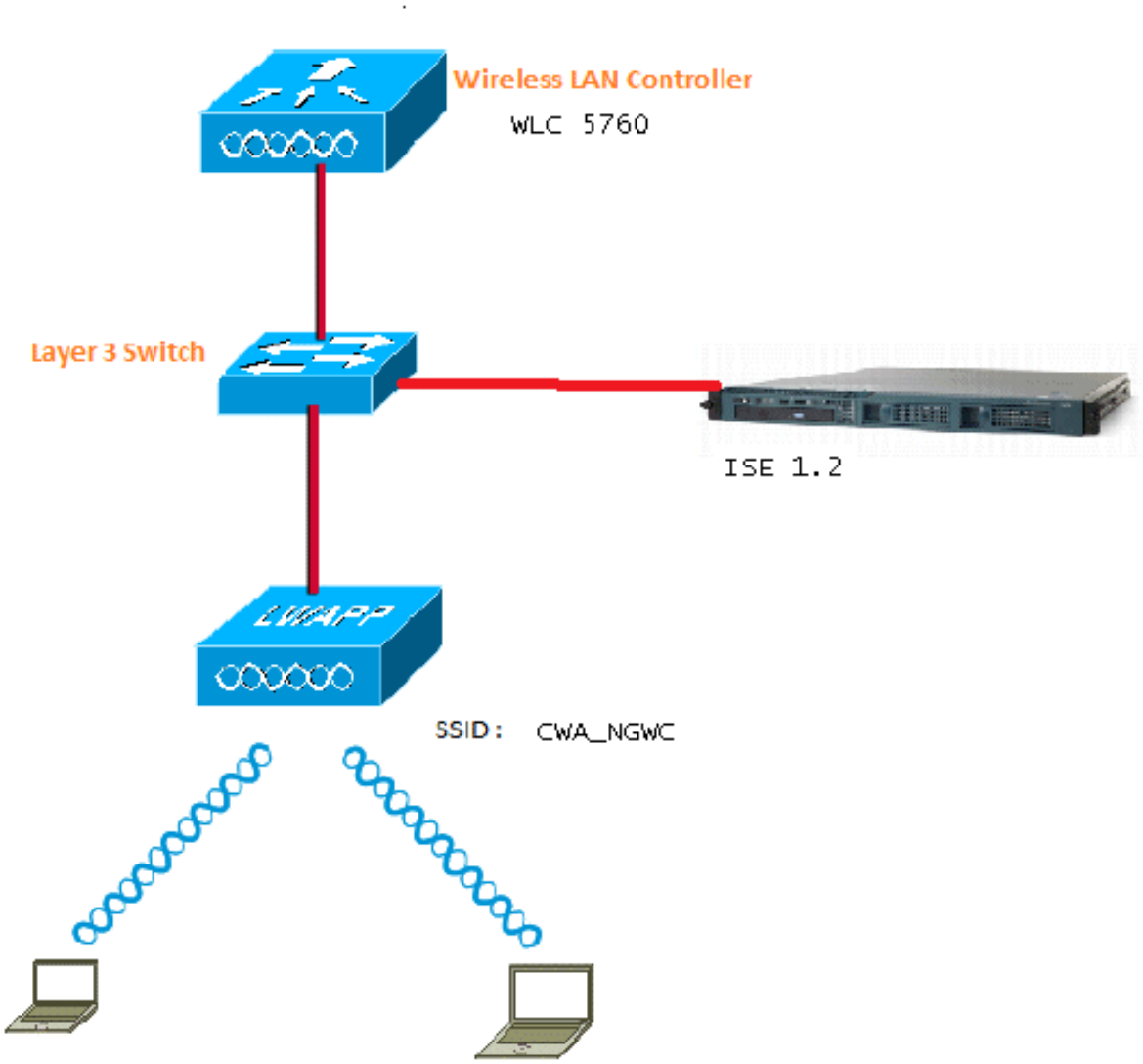
플로우에는 다음 단계가 포함됩니다.

1. 사용자가 웹 인증 SSID(Service Set Identifier)에 연결합니다. 이 SSID는 사실상 open+macfiltering이며 Layer 3 보안은 없습니다.
2. 사용자가 브라우저를 엽니다.
3. WLC가 게스트 포털로 리디렉션됩니다.
4. 사용자가 포털에서 인증합니다.
5. ISE는 RADIUS CoA(Change of Authorization)(CoA - UDP 포트 1700)를 컨트롤러로 전송하여 사용자가 유효함을 표시하며, 결국 ACL(Access Control List)과 같은 RADIUS 특성을 푸시합니다.
6. 사용자에게 원래 URL을 다시 시도하라는 메시지가 표시됩니다.

Cisco는 CWA(Central Web Authentication)를 수행하기 위해 다양한 시나리오를 모두 다루는 세 가지 구축 설정을 사용합니다.

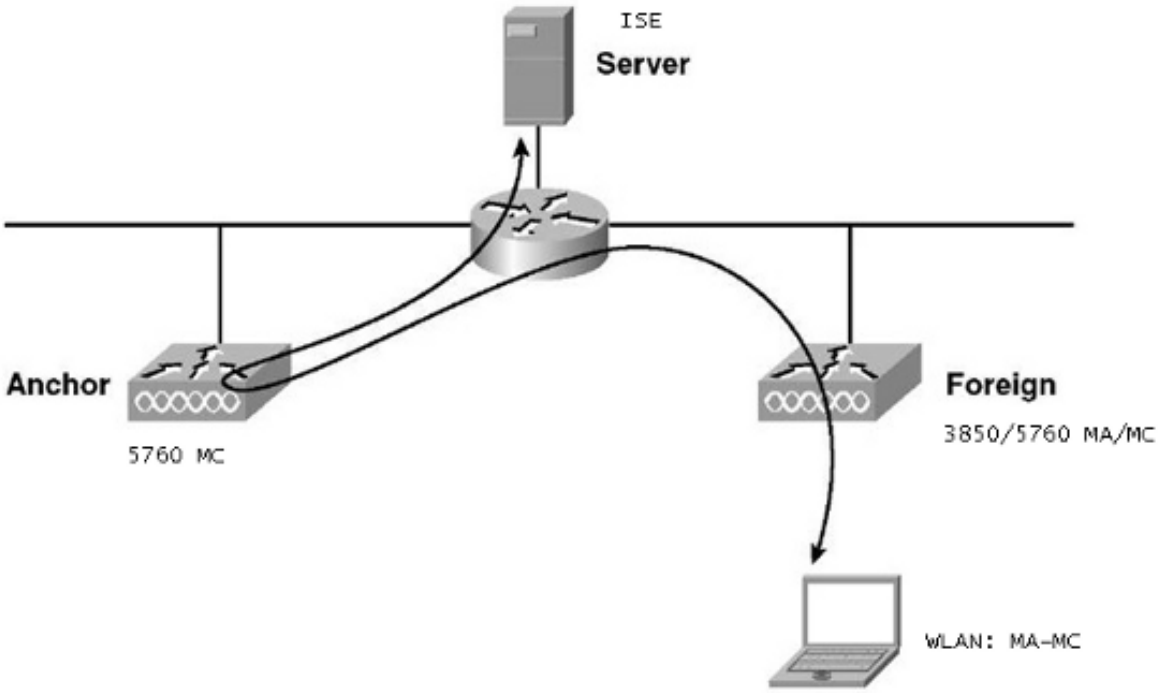
토폴로지 1

5760 WLC는 독립형 WLC의 역할을 하며 액세스 포인트는 동일한 5760 WLC에서 종료됩니다. 클라이언트는 WLAN(Wireless LAN)에 연결되며 ISE에 인증됩니다.



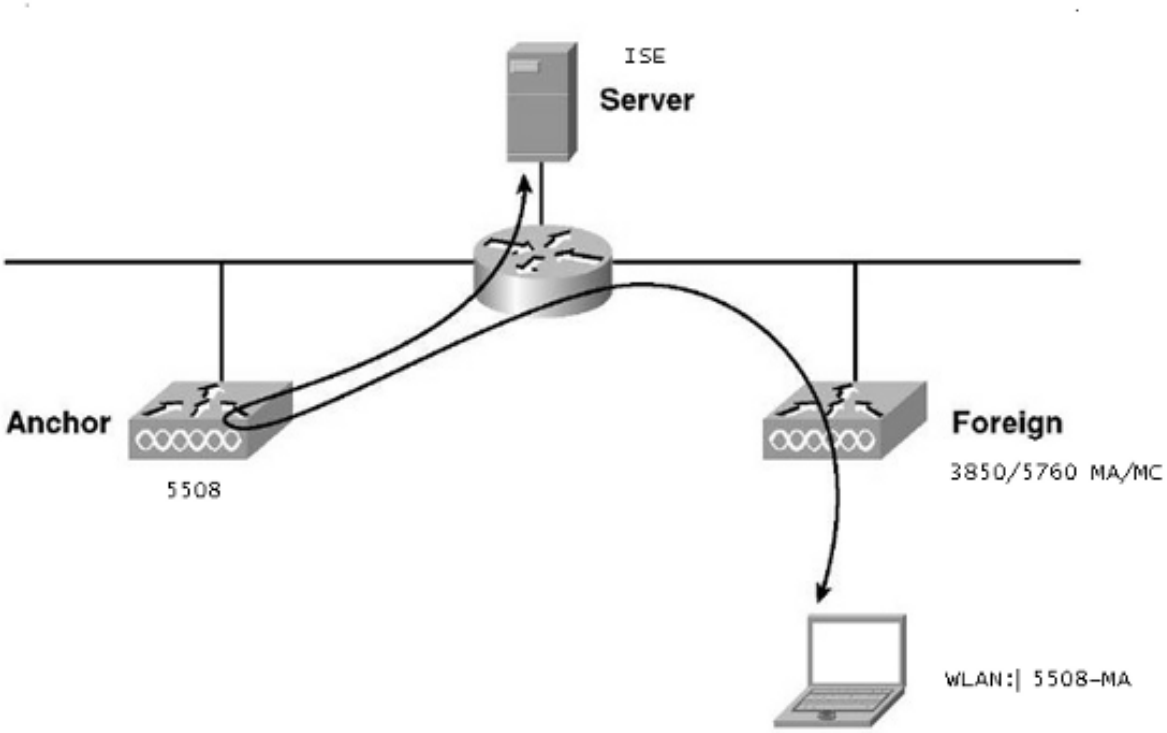
토폴로지 2

모빌리티 컨트롤러 역할을 하는 WLC와 모빌리티 에이전트 역할을 하는 WLC 간의 게스트 고정 모빌리티 에이전트는 외부 WLC이고 모빌리티 컨트롤러는 앵커입니다.



토폴로지 3

Cisco Unified WLC 5508과 Converged Access WLC 5760/3850 사이에 게스트 고정 기능을 제공하는 데 하나는 모빌리티 컨트롤러 역할을 하고 다른 하나는 모빌리티 에이전트 역할을 합니다. Mobility Agent/Mobility Controller는 외부 WLC이고 5508 Mobility Controller는 앵커입니다.



참고: 앵커가 모빌리티 컨트롤러이고 외부 WLC가 다른 모빌리티 컨트롤러에서 라이센스를 가져오는 모빌리티 에이전트인 구축이 많습니다. 이 경우 외부 WLC에는 앵커가 하나만 있으며 해당 앵커가 정책을 푸시합니다. 이중 앵커링은 지원되지 않으며, 그렇게 작동하지 않을 것으로 예상되므로 작동하지 않는다.

예

WLC 5508은 앵커 역할을 하고 WLC 5760은 모빌리티 에이전트 역할을 하는 3850 스위치의 모빌리티 컨트롤러 역할을 합니다. 앵커 외부 WLAN의 경우 WLC 5508이 3850 외부 WLAN의 앵커가 됩니다. WLC 5760에서 해당 WLAN을 구성할 필요가 없습니다. 3850 스위치를 5760 앵커로 가리킨 다음 이 WLC 5760에서 WLC 5508을 이중 앵커로 지정하면 이중 앵커링이 되고 정책이 5508 앵커에 있으므로 작동하지 않습니다.

WLC 5508을 앵커로, WLC 5760을 모빌리티 컨트롤러로, 3850 스위치를 모빌리티 에이전트 및 외부 WLC로 포함하는 설정이 있는 경우 언제든지 3850 스위치의 앵커가 WLC 5760 또는 WLC 5508이 됩니다. 동시에 둘 다 같을 수 없고 이중 앵커는 작동하지 않습니다.

토폴로지 1 컨피그레이션 예

네트워크 다이어그램 및 설명은 토폴로지 1을 참조하십시오.

구성은 2단계 프로세스입니다.

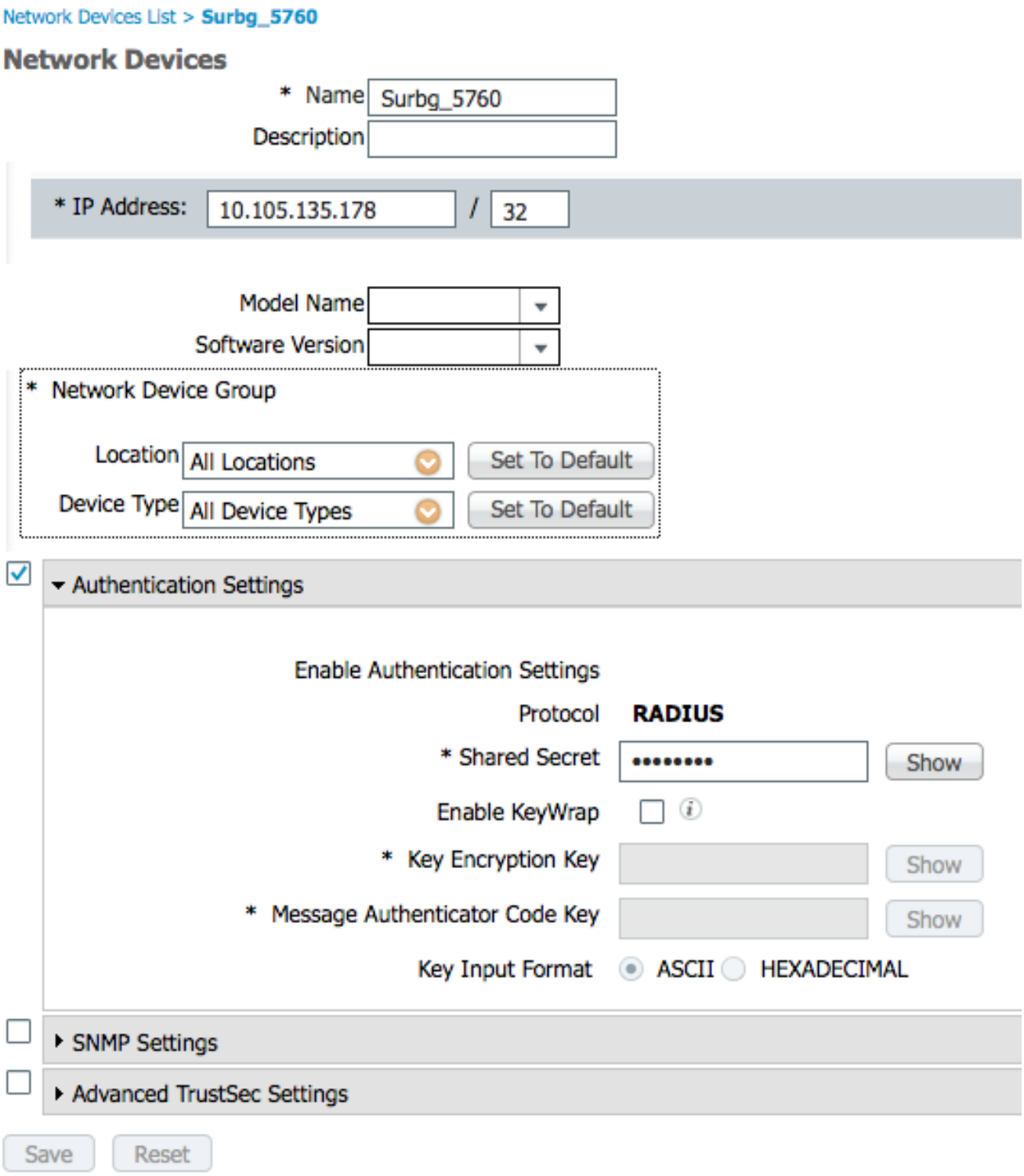
1. ISE의 컨피그레이션입니다.
2. WLC의 컨피그레이션.

WLC 5760은 독립형 WLC의 역할을 하며 사용자는 ISE에 인증됩니다.

ISE의 컨피그레이션

1. ISE의 **WLC를** AAA(Authentication, Authorization, and Accounting) 클라이언트로 추가하려면 ISE **GUI > Administration > Network Resource > Network Devices List > Add**를 선택합니다. RADIUS 서버에 추가된 WLC에 동일한 공유 암호를 입력해야 합니다. **참고**: Anchor-Foreign을 구축하는 동안에는 외부 WLC만 추가하면 됩니다. ISE에서 앵커 WLC를 AAA 클라이언트로 추가할 필요가 없습니다. 이 문서의 다른 모든 구축 시나리오에는 동일한 ISE 컨피그레이션이 사용됩니다

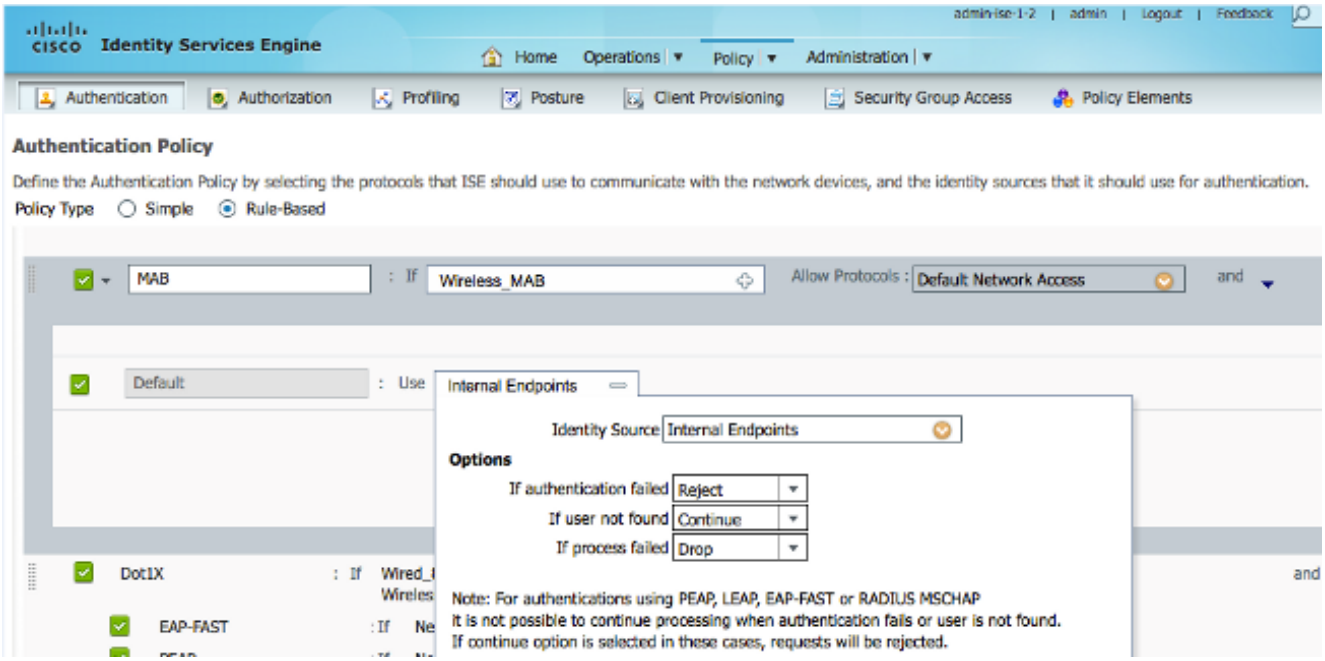
.



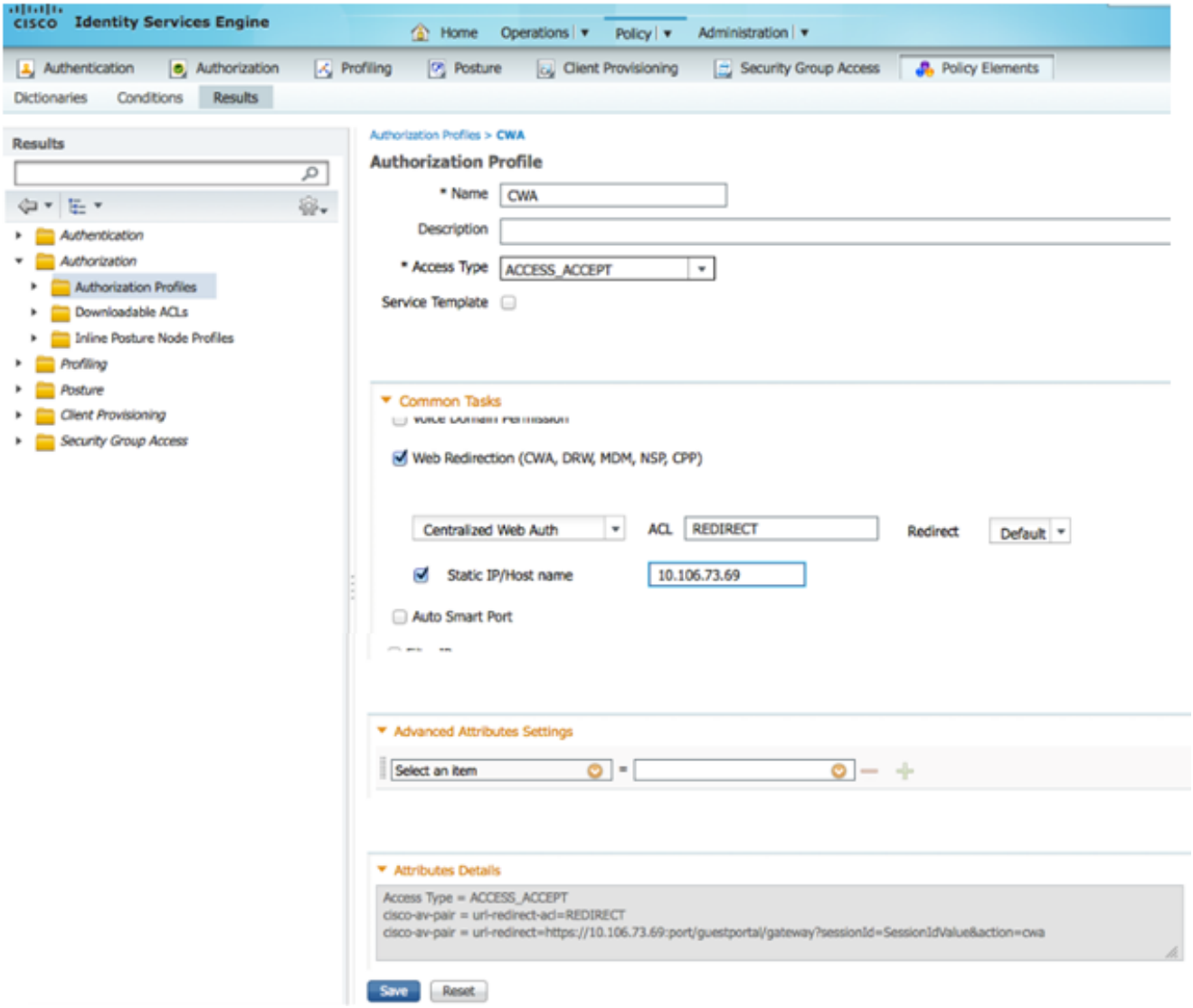
2. 인증 정책을 생성하려면 ISE GUI에서 **Policy(정책) > Authentication(인증) > MAB >** Edit(수정)를 선택합니다. 인증 정책은 내부 엔드 포인트를 가리키는 클라이언트의 MAC 주소를 수락 합

니다. 옵션 목록에서 다음 선택 사항을 선택합니다.If authentication failed(인증에 실패한 경우) 드롭다운 목록에서 Reject(**거부**)를 **선택합니다**.사용자를 찾을 수 없는 경우 드롭다운 목록에서 계속을 **선택합니다**.If process failed(프로세스가 실패한 경우) 드롭다운 목록에서 Drop(삭제)**을 선택합니다**.이러한 옵션으로 구성할 경우 MAC 권한 부여에 실패한 클라이언트는 게스트 포털을 진행합니다

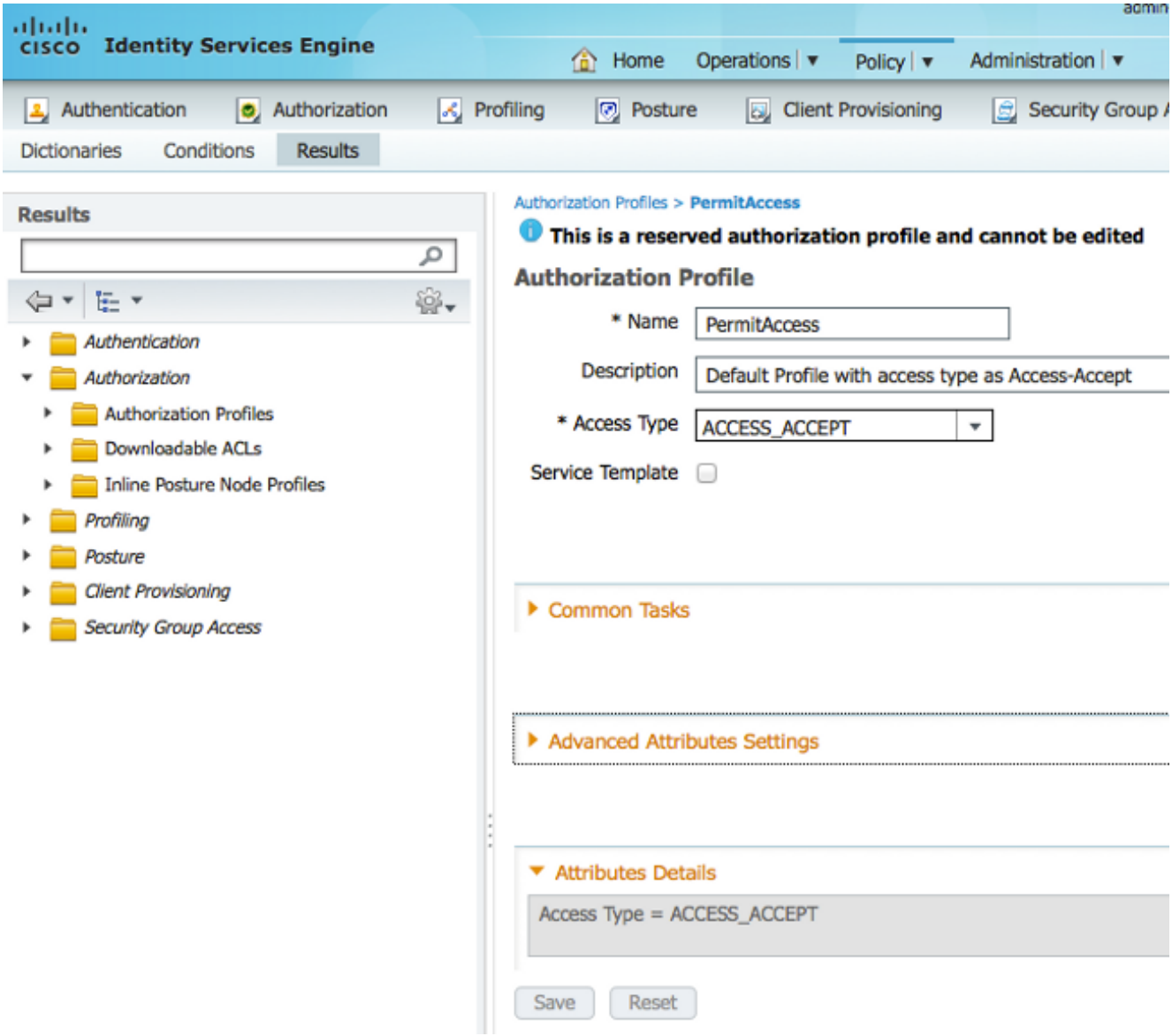
.



3. ISE GUI에서 **Policy(정책) > Authorization(권한 부여) > Results(결과) > Authorization Profiles(권한 부여 프로파일) > Add(추가)를** 선택합니다. 세부사항을 입력하고 Save(**저장**)를 클릭하여 Authorization 프로파일을 생성합니다. 이 프로파일은 클라이언트가 게스트 사용자 이름/비밀번호를 입력하는 MAC 인증 후 리디렉션 URL로 리디렉션되도록 도와줍니다.

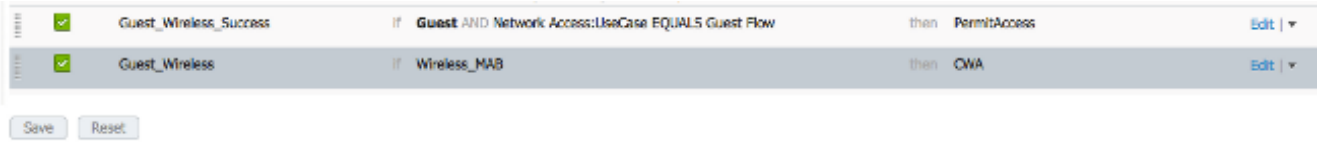


4. ISE GUI에서 **Policy(정책) > Authorization(권한 부여) > Results(결과) > Authorization Profiles(권한 부여 프로파일) > Add(추가)**를 선택하여 다른 권한 부여 프로파일을 생성하여 올바른 자격 증명으로 사용자에 대한 액세스를 허용합니다.



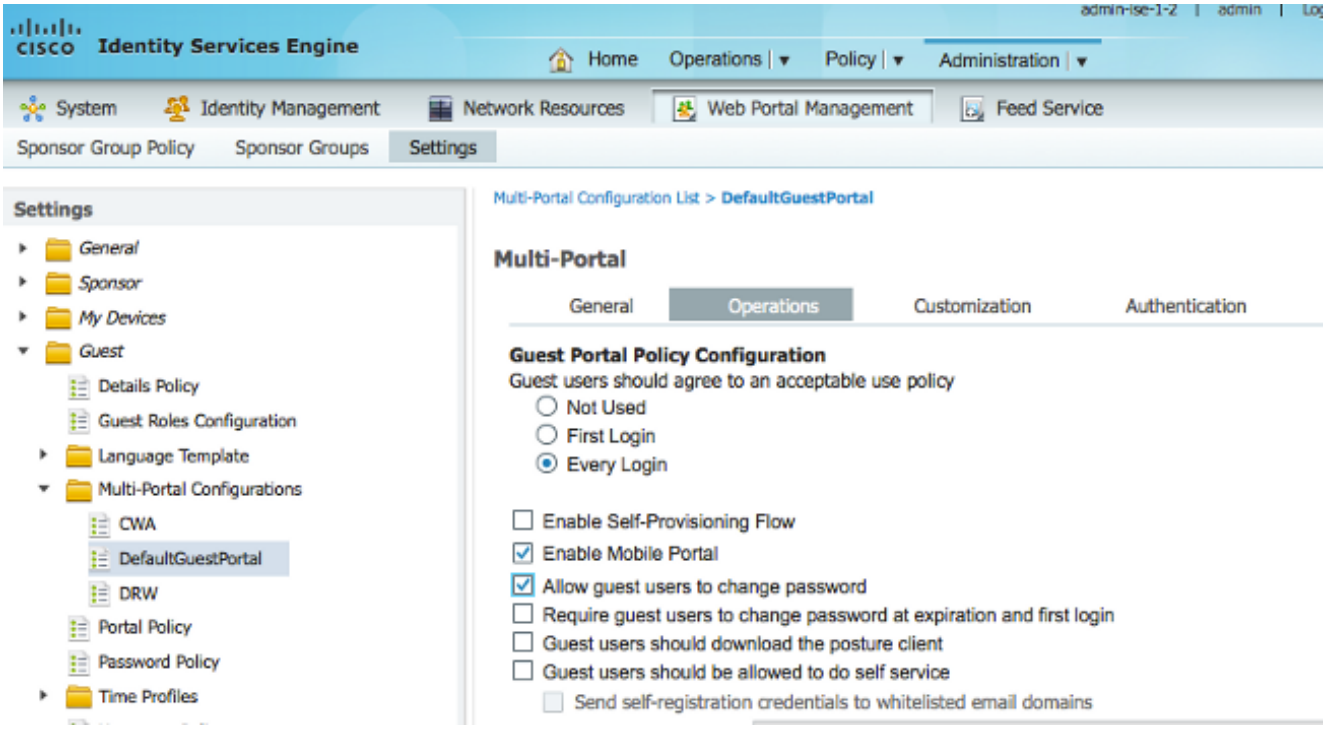
5. 권한 부여 정책을 생성합니다. 권한 부여 정책 'Guest_Wireless'는 리디렉션 URL 및 리디렉션 ACL을 클라이언트 세션에 푸시합니다. 여기에 푸시된 프로파일은 앞서 표시된 대로 CWA입니다.권한 부여 정책 'Guest_Wireless-Success'는 게스트 포털을 통해 성공적으로 인증된 게스트 사용자에게 전체 액세스 권한을 부여합니다. 사용자가 게스트 포털에서 성공적으로 인증되면 WLC에 의해 동적 권한 부여가 전송됩니다. 이렇게 하면 'Network Access:Usecase EQUALS Guest Flow' 특성을 사용하여 클라이언트 세션이 재인증됩니다.최종 권한 부여 정책은 다음과 같습니다

.



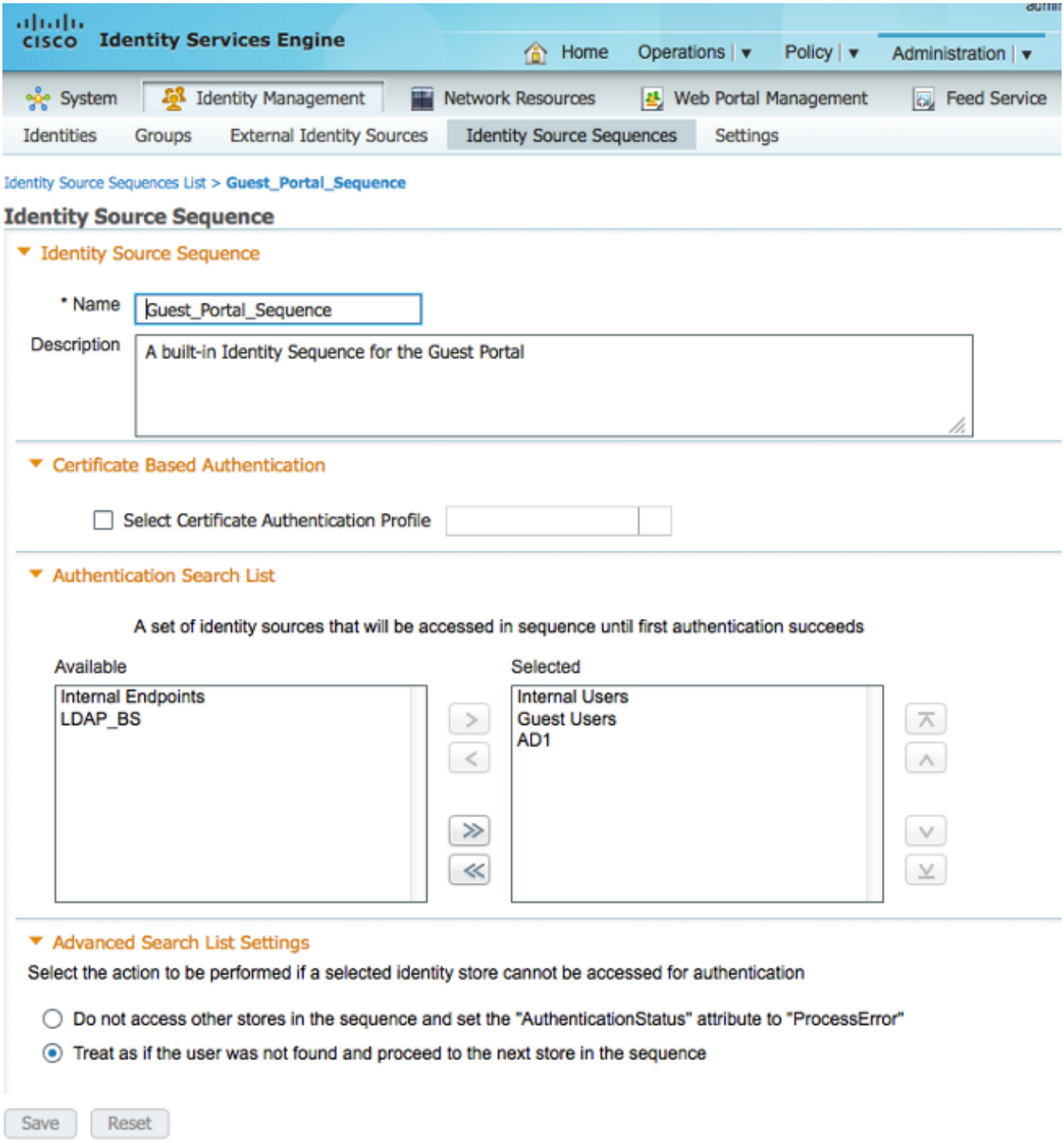
6. 선택 사항: 이 경우 기본 다중 포털 컨피그레이션이 사용됩니다. 요구 사항에 따라 GUI에서 동일한 사항을 변경할 수 있습니다. ISE GUI에서 Administration(관리) > **Web Portal management(웹 포털 관리) > Multi Portal Configurations(다중 포털 컨피그레이션) > DefaultGuestPortal(기본 게스트 포털)을** 선택합니다

.

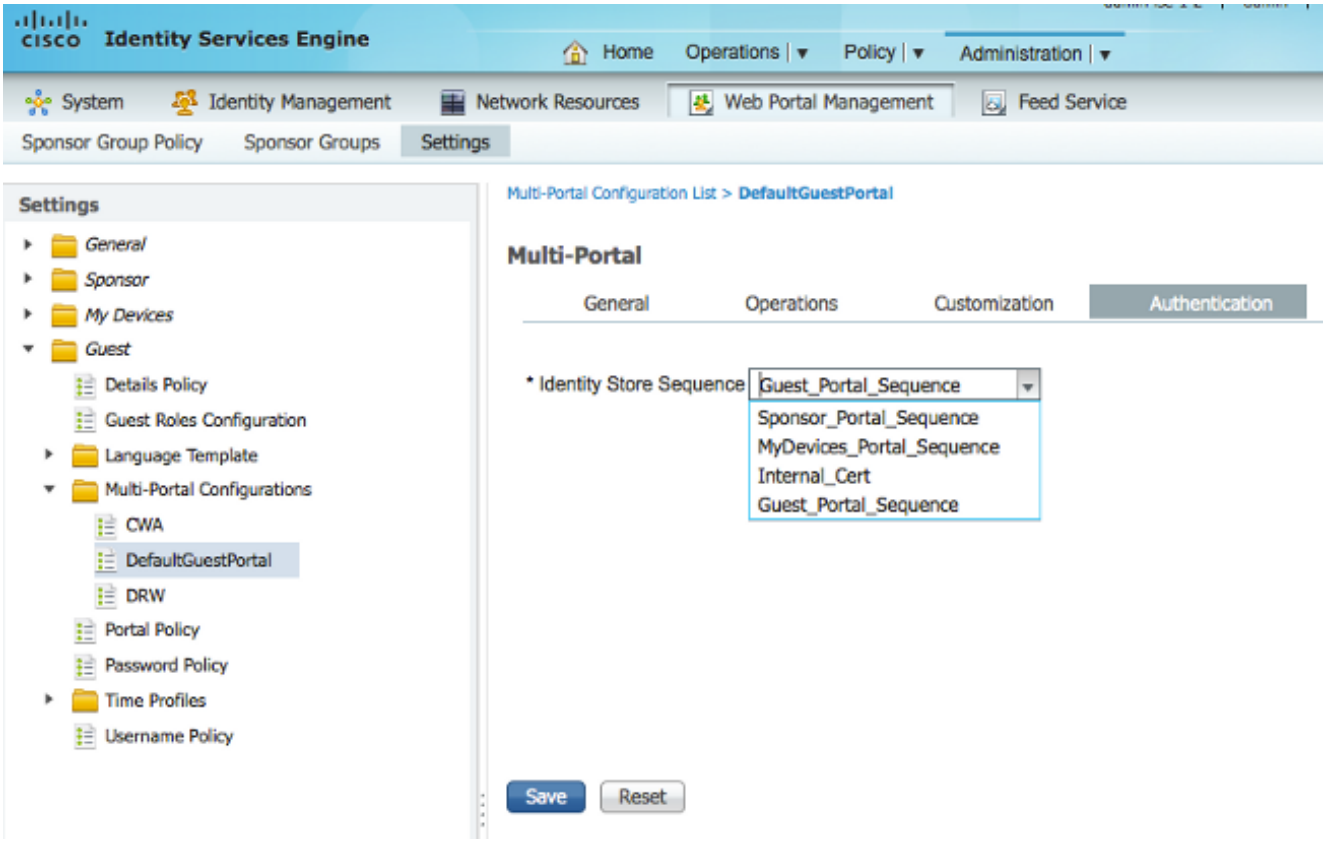


내부, 게스트 및 AD 사용자를 허용하는 Guest_Portal_sequence가 생성됩니다

.



7. ISE GUI에서 **Guest(게스트) > Multi-Portal Configurations(다중 포털 컨피그레이션) > DefaultGuestPortal(기본 게스트 포털)을** 선택합니다. Identify Store Sequence(스토어 시퀀스 식별) 드롭다운 목록에서 **Guest_Portal_Sequence를** 선택합니다.



WLC의 컨피그레이션

1. WLC 5760에서 ISE Radius 서버를 정의합니다.
2. CLI를 사용하여 RADIUS 서버, 서버 그룹 및 방법 목록을 구성합니다.

```
dot1x system-auth-control

radius server ISE
address ipv4 10.106.73.69 auth-port 1645 acct-port 1646
 timeout 10
 retransmit 3
 key Cisco123


aaa group server radius ISE
server name ISE
deadtime 10

aaa authentication dot1x ISE group ISE
aaa authorization network ISE group ISE

aaa authorization network MACFILTER group ISE
aaa accounting identity ISE start-stop group ISE
!

aaa server radius dynamic-author
client 10.106.73.69 server-key Cisco123
auth-type any
```

3. CLI를 사용하여 WLAN을 구성합니다.

```
wlan CWA_NGWC 10 CWA_NGWC
 aaa-override
accounting-list ISE
client vlan VLAN0012
no exclusionlist
mac-filtering MACFILTER
nac
```

```
no security wpa
no security wpa akm dot1x
no security wpa wpa2
 no security wpa wpa2 ciphers aes
 security dot1x authentication-list ISE
 session-timeout 1800
 no shutdown
```

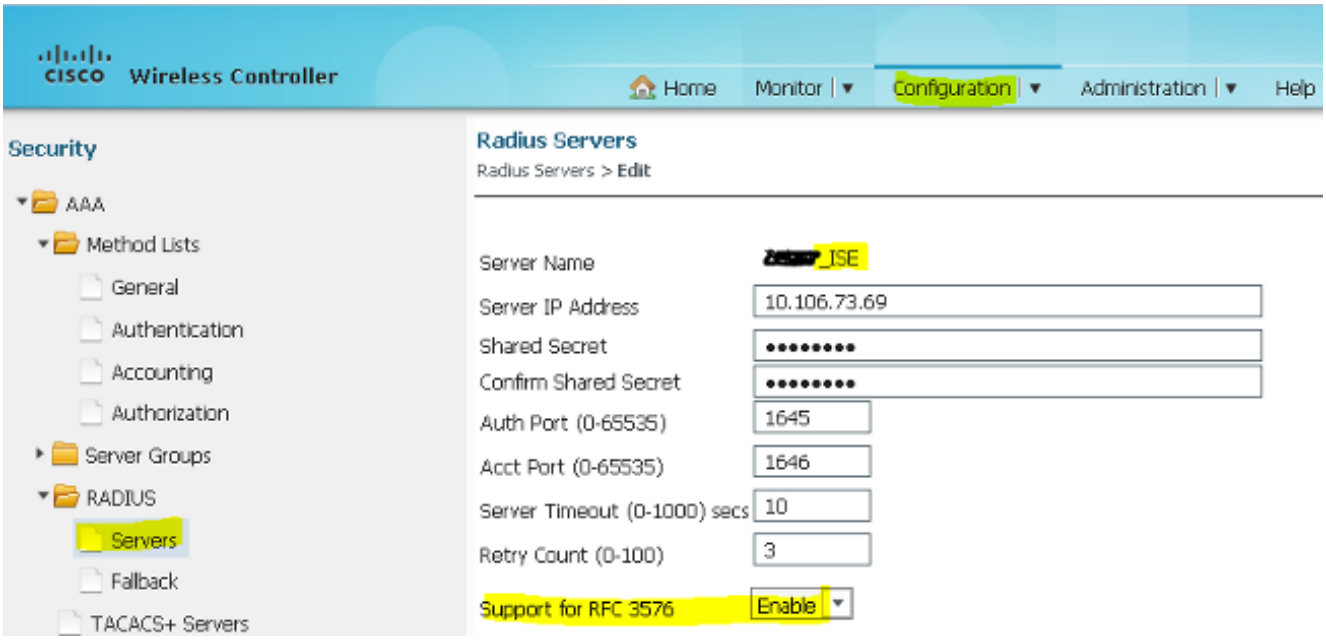
4. CLI로 리디렉션 ACL을 구성합니다. 이는 ISE가 게스트 포털 리디렉션을 위한 리디렉션 URL과 함께 AAA 재정의로 반환하는 url-redirect-acl입니다. 현재 통합 아키텍처에서 사용되는 직접 ACL입니다. 이는 'punt' ACL로, Unified Architecture에 일반적으로 사용하는 일종의 역방향 ACL입니다. DHCP, DHCP 서버, DNS, DNS 서버 및 ISE 서버에 대한 액세스를 차단해야 합니다. 필요에 따라 www, 443 및 8443만 허용합니다. 이 ISE 게스트 포털에서는 포트 8443을 사용하며 리디렉션은 여기에 표시된 ACL에서 계속 작동합니다. 여기서 ICMP가 활성화되지만 보안 규칙에 따라 거부 또는 허용할 수 있습니다.

```
ip access-list extended REDIRECT
 deny icmp any any
 deny udp any any eq bootps
 deny udp any any eq bootpc
 deny udp any any eq domain
deny ip any host 10.106.73.69
 permit tcp any any eq www
 permit tcp any any eq 443
```

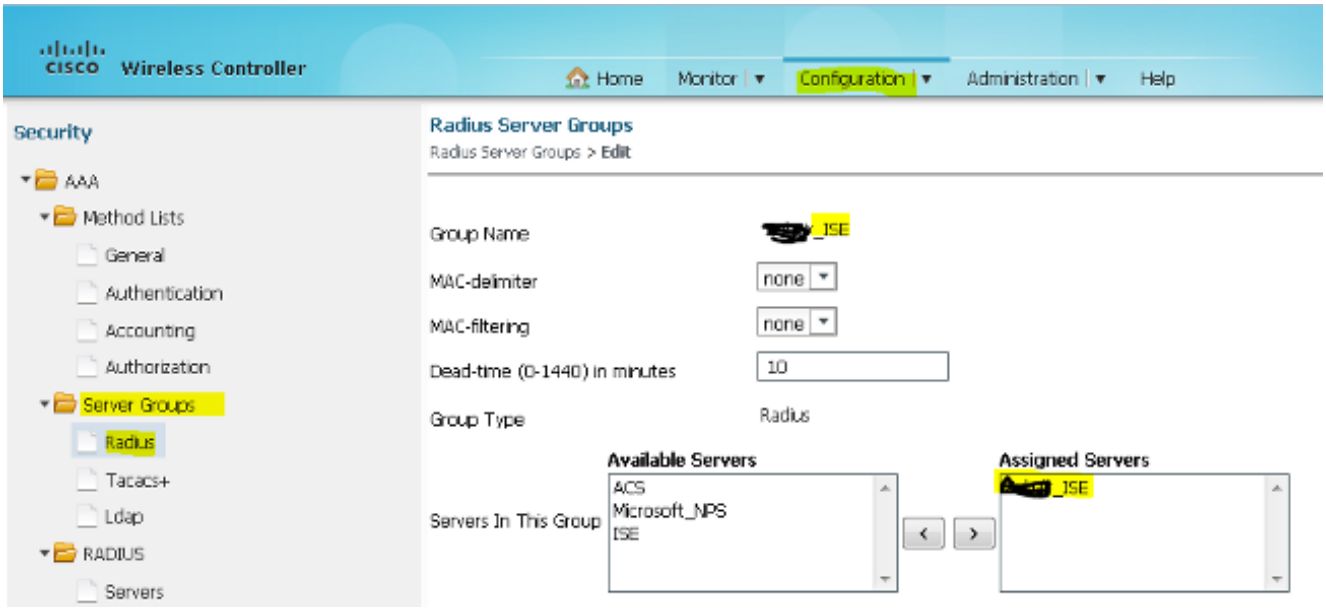
주의: HTTPS를 활성화하면 확장성으로 인해 일부 높은 CPU 문제가 발생할 수 있습니다. Cisco 설계 팀에서 권장하지 않는 한 이 옵션을 활성화하지 마십시오.

5. Wireless Controller GUI에서 **AAA > RADIUS > Servers를** 선택합니다. GUI에서 RADIUS 서버, 서버 그룹 및 방법 목록을 구성합니다. 모든 매개변수를 채우고 여기에 구성된 공유 암호가 이 디바이스에 대해 ISE에 구성된 공유 암호와 일치하는지 확인합니다. Support for RFC 3576(RFC 3576 지원) 드롭다운 목록에서 Enable(활성화)**을 선택합니다**

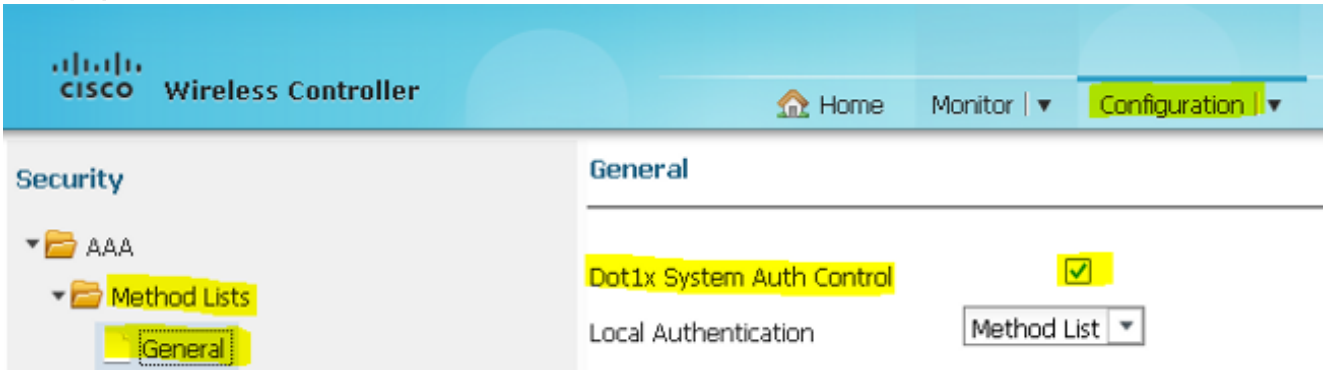
.



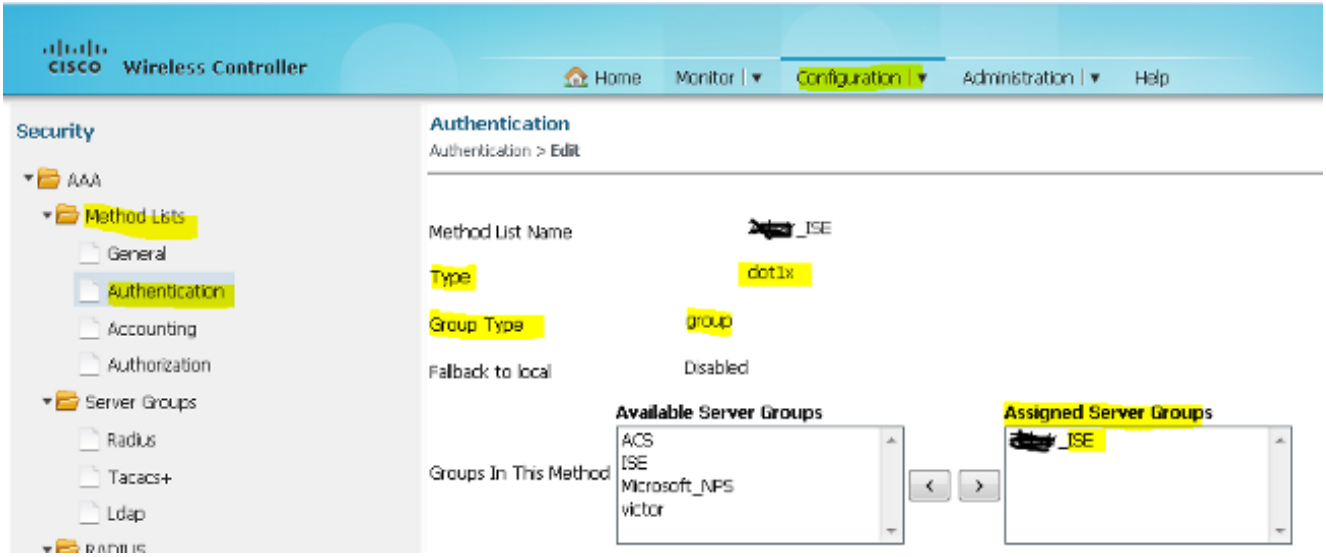
6. Wireless Controller GUI에서 **AAA > Server Groups > Radius를** 선택합니다. 이전에 생성한 RADIUS 서버를 서버 그룹에 추가합니다.



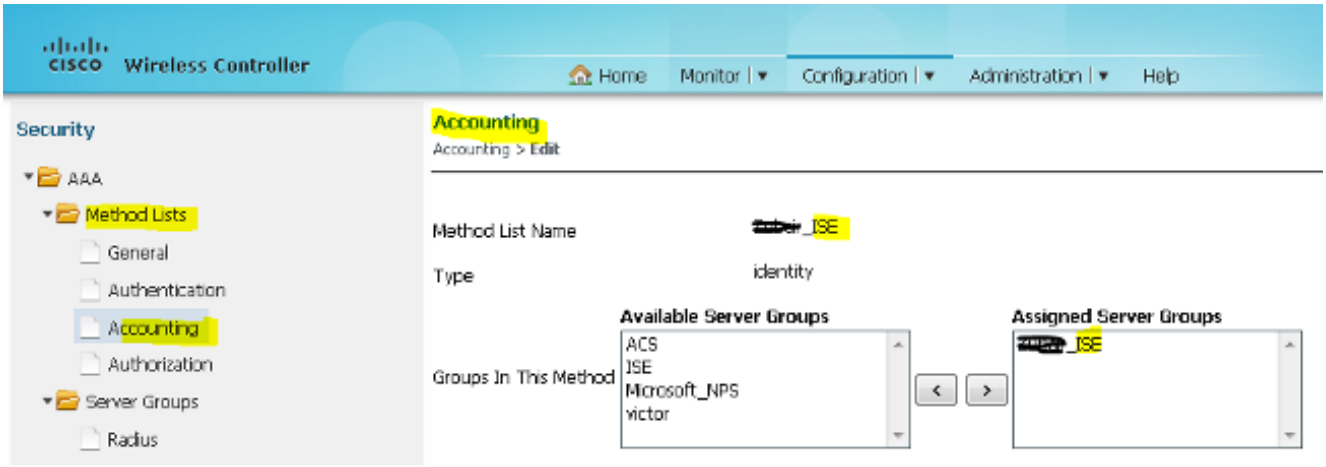
7. Wireless Controller GUI에서 **AAA > Method Lists > General을** 선택합니다. Dot**1x 시스템 인증 제어 확인란**을 선택합니다. 이 옵션을 비활성화하면 AAA가 작동하지 않습니다.



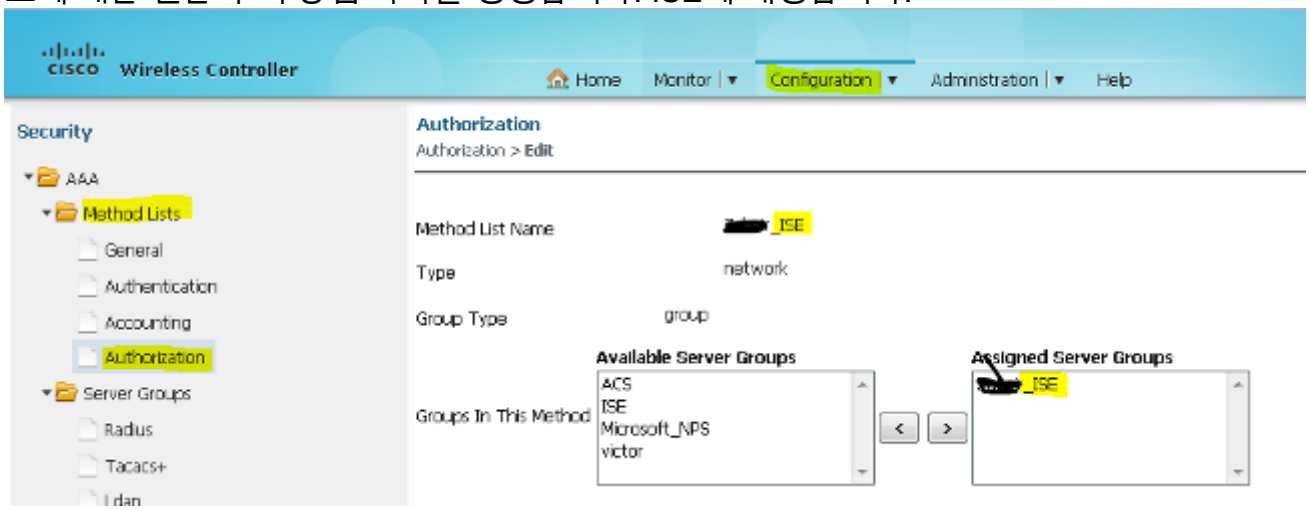
8. Wireless Controller GUI에서 **AAA > Method Lists > Authentication을** 선택합니다. Type dot1X에 대한 인증 방법 목록을 만듭니다. 그룹 유형은 그룹입니다. ISE에 매핑합니다.



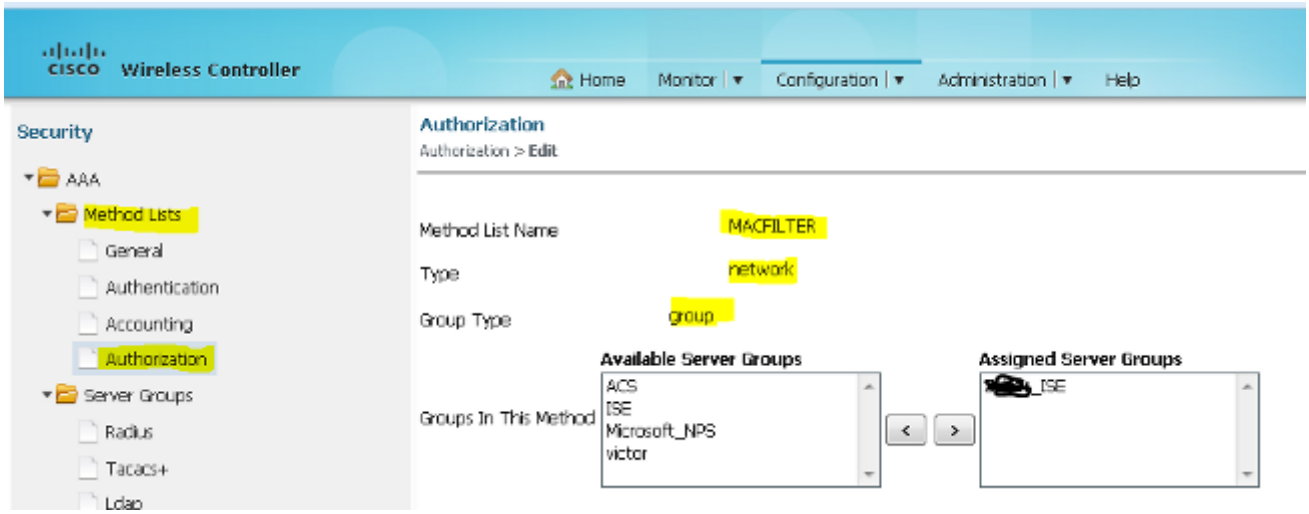
9. Wireless Controller GUI에서 **AAA > Method Lists > Accounting을** 선택합니다. 유형 ID에 대한 계정 관리 방법 목록을 만듭니다. ISE에 매핑합니다.



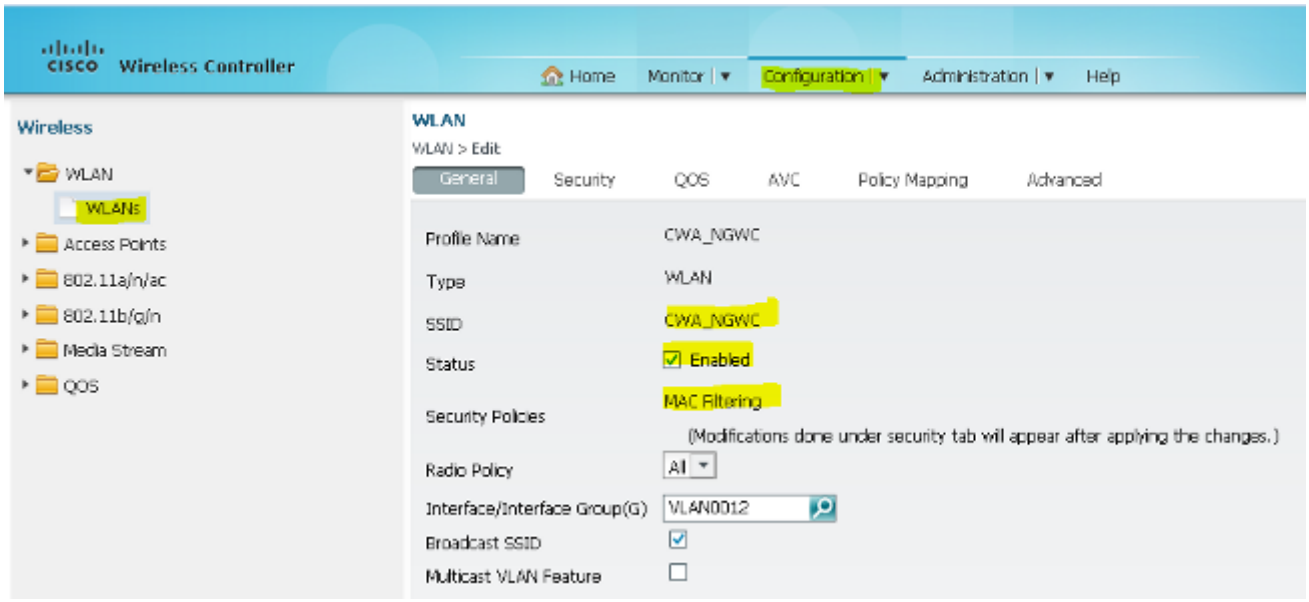
10. Wireless Controller GUI에서 **AAA > Method Lists > Authorization**을 선택합니다. 유형 네트워크에 대한 권한 부여 방법 목록을 생성합니다. ISE에 매핑합니다.



11. 장애 지원에도 MAC이 있으므로 선택 사항입니다. 유형 네트워크에 대한 권한 부여 방법 목록 MACFILTER를 만듭니다. ISE에 매핑합니다.

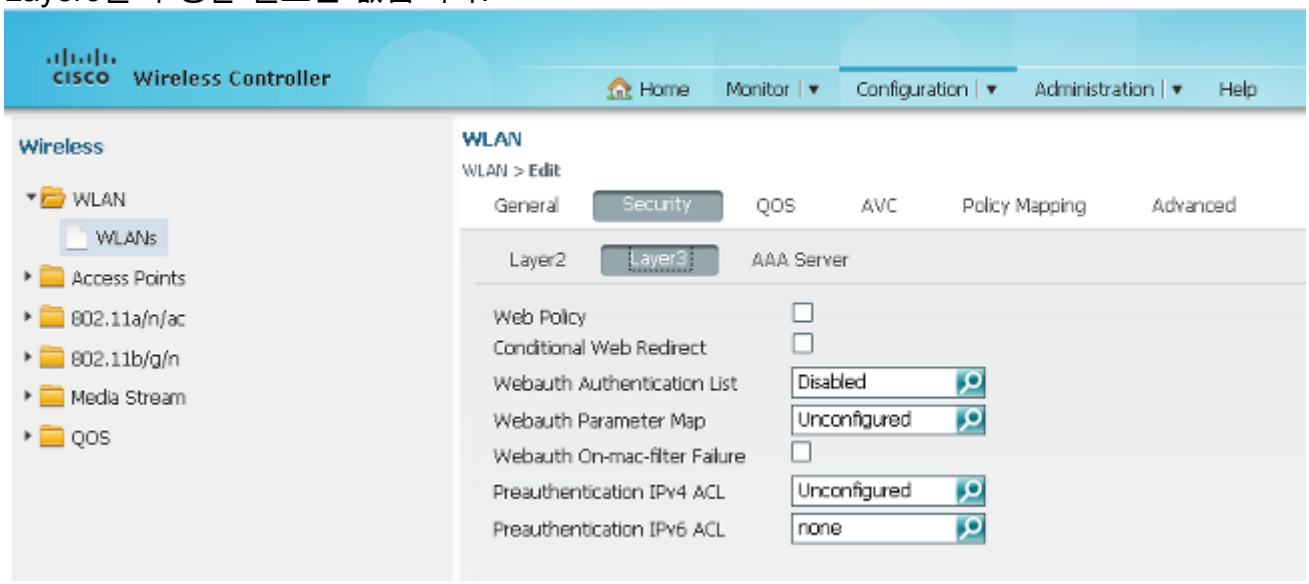


12. Wireless Controller GUI에서 WLAN(WLAN) **> WLANs(WLAN)**를 선택합니다. 여기에 표시된 매개변수를 사용하여 새 컨피그레이션을 생성합니다.

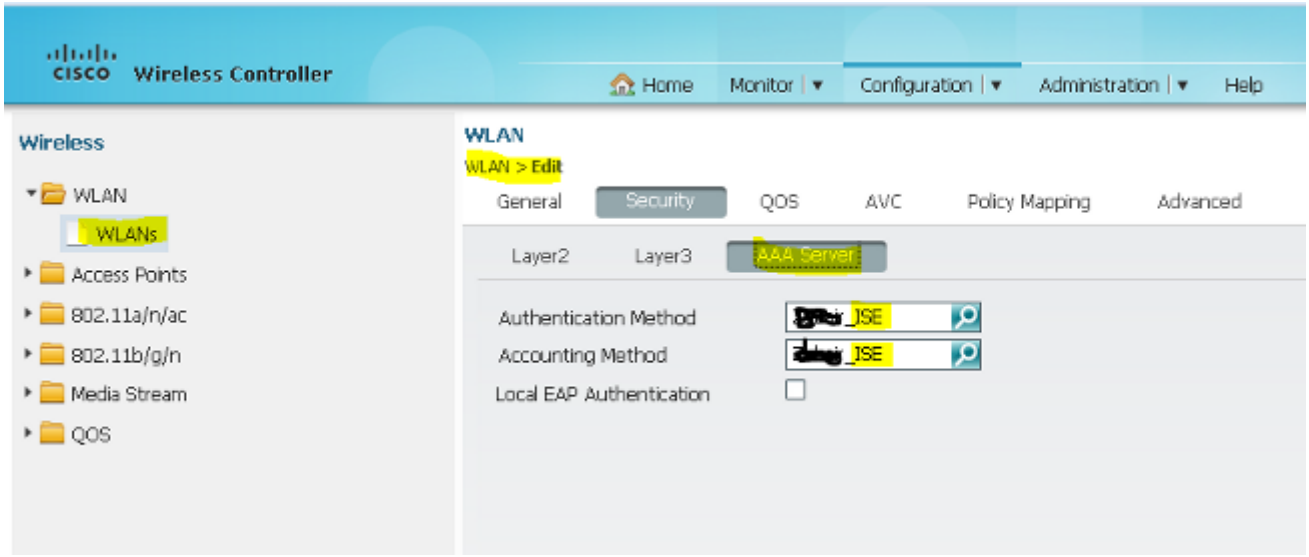


13. Security(**보안**) **> Layer2를 선택합니다**. MAC Filtering(MAC 필터링) 필드에 MACFILTER**를 입력합니다**.

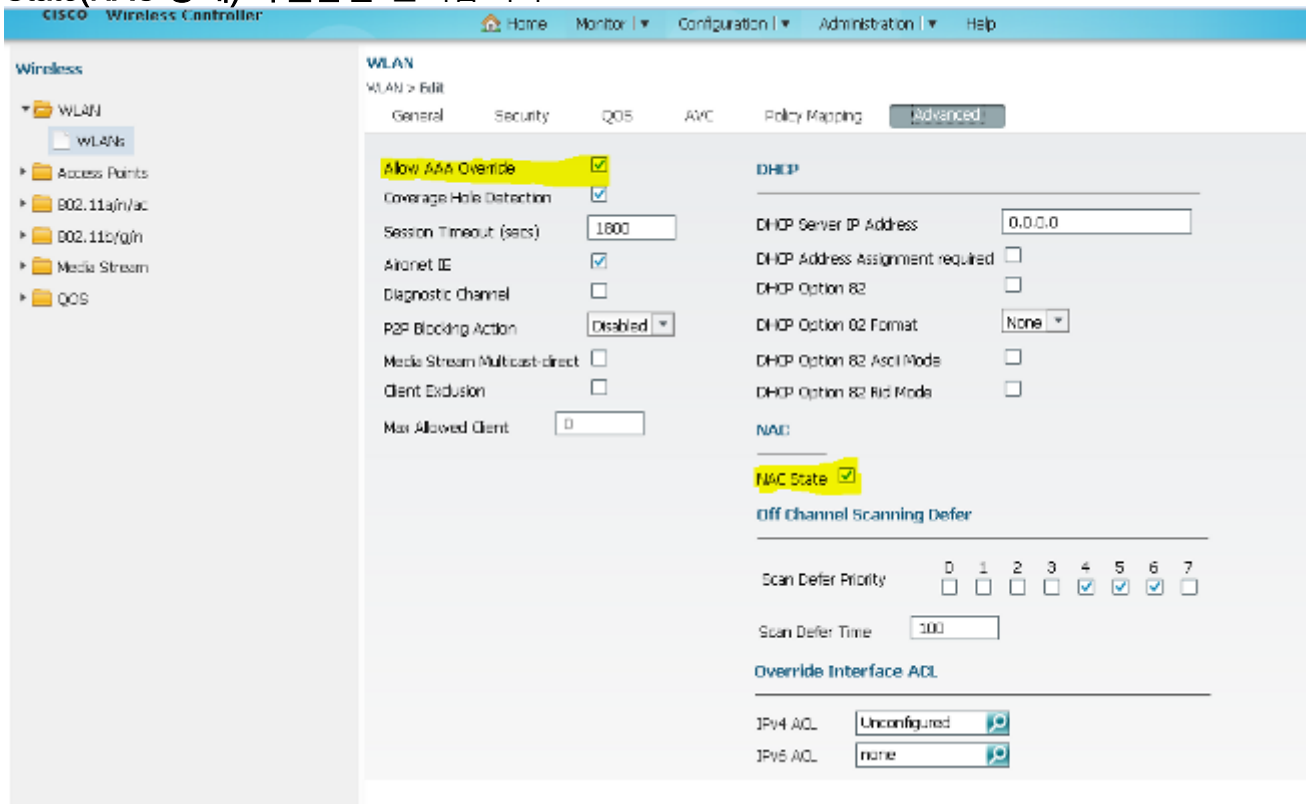
14. Layer3를 구성할 필요는 없습니다.



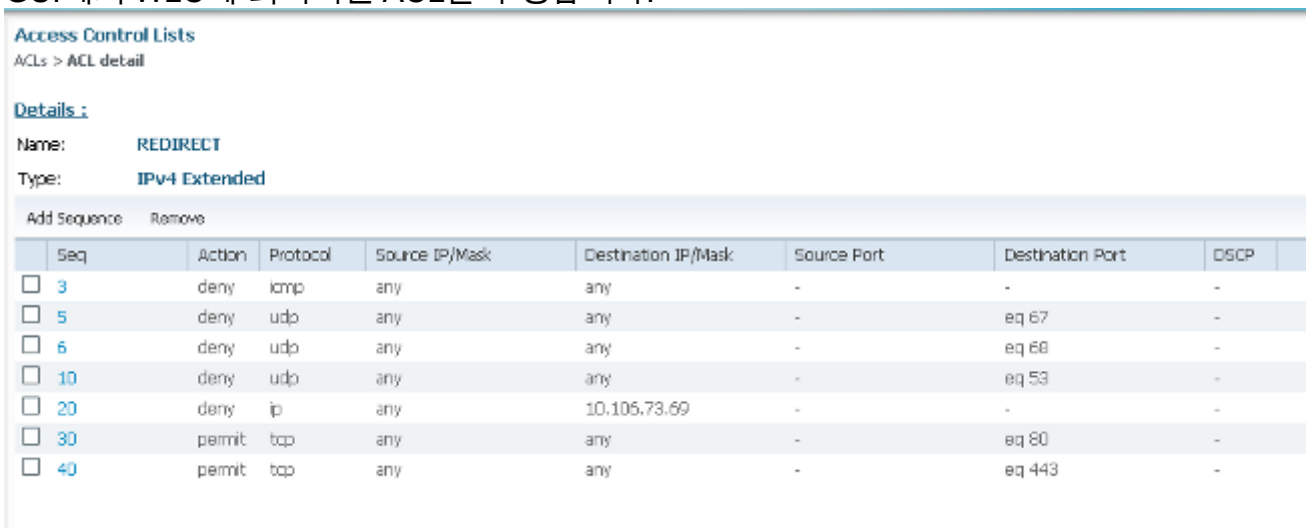
15. Security(**보안**) **> AAA Server(AAA 서버)를 선택합니다**. Authentication Method(인증 방법) 드롭다운 목록에서 ISE를 **선택합니다**. Accounting Method(어카운팅 방법) 드롭다운 목록에서 **ISE**를 선택합니다.



16. 고급을 **선택합니다**. Allow **AAA Override(AAA 재정의 허용)** 확인란을 선택합니다. **NAC State(NAC 상태) 확인란**을 선택합니다.



17. GUI에서 WLC에 리디렉션 ACL을 구성합니다.



Seq	Action	Protocol	Source IP/Mask	Destination IP/Mask	Source Port	Destination Port	DSCP
3	deny	icmp	any	any	-	-	-
5	deny	udp	any	any	-	eq 67	-
6	deny	udp	any	any	-	eq 68	-
10	deny	udp	any	any	-	eq 53	-
20	deny	ip	any	10.105.73.69	-	-	-
30	permit	tcp	any	any	-	eq 80	-
40	permit	tcp	any	any	-	eq 443	-

토폴로지 2 컨피그레이션 예

네트워크 다이어그램 및 설명은 토폴로지 2를 참조하십시오.

이 컨피그레이션도 2단계 프로세스입니다.

ISE의 컨피그레이션

ISE의 컨피그레이션은 토폴로지 1 컨피그레이션과 동일합니다.

ISE에 Anchor Controller를 추가할 필요가 없습니다. ISE에 외부 WLC를 추가하고, 외부 WLC에서 RADIUS 서버를 정의하고, WLAN에 권한 부여 정책을 매핑하기만 하면 됩니다. 앵커에서는 MAC 필터링을 활성화하기만 하면 됩니다.

이 컨피그레이션 예에는 앵커 외래 역할을 하는 두 개의 WLC 5760이 있습니다. WLC 5760을 앵커로 사용하고 3850 스위치를 Anchor Foreign(모빌리티 에이전트)으로 사용하여 다른 모빌리티 컨트롤러로 사용하려는 경우 동일한 컨피그레이션이 정확합니다. 그러나 3850 스위치에서 라이센스를 가져오는 두 번째 모빌리티 컨트롤러에서 WLAN을 구성할 필요는 없습니다. 3850 스위치를 앵커 역할을 하는 WLC 5760에 연결하기만 하면 됩니다.

WLC의 컨피그레이션

1. Foreign(외부)에서 AAA에 대한 AAA Method(AAA 방법) 목록을 사용하여 ISE 서버를 구성하고 WLAN을 MAC 필터 권한 부여에 매핑합니다. **참고**: 앵커 및 외부 모두와 MAC 필터링에서 리디렉션 ACL을 구성합니다.

```
dot1x system-auth-control

radius server ISE
 address ipv4 10.106.73.69 auth-port 1645 acct-port 1646
 timeout 10
 retransmit 3
 key Cisco123


aaa group server radius ISE
 server name ISE
 deadtime 10


aaa authentication dot1x ISE group ISE

aaa authorization network ISE group ISE

aaa authorization network MACFILTER group ISE
aaa accounting identity ISE start-stop group ISE
!

aaa server radius dynamic-author
 client 10.106.73.69 server-key Cisco123
 auth-type any

wlan MA-MC 11 MA-MC
 aaa-override
 accounting-list  ISE
 client vlan VLAN0012
 mac-filtering MACFILTER
```

```
 mobility anchor 10.105.135.244
nac
 no security wpa
 no security wpa akm dot1x
 no security wpa wpa2
 no security wpa wpa2 ciphers aes
security dot1x authentication-list ISE
 session-timeout 1800
 no shutdown
```

2. CLI로 리디렉션 ACL을 구성합니다. 이는 ISE가 게스트 포털 리디렉션을 위한 리디렉션 URL과 함께 AAA 재정의로 반환하는 url-redirect-acl입니다. 현재 통합 아키텍처에서 사용되는 직접 ACL입니다. 이는 'punt' ACL로, Unified Architecture에 일반적으로 사용하는 일종의 역방향 ACL입니다. DHCP, DHCP 서버, DNS, DNS 서버 및 ISE 서버에 대한 액세스를 차단해야 합니다. 필요에 따라 www, 443 및 8443만 허용합니다. 이 ISE 게스트 포털에서는 포트 8443을 사용하며 리디렉션은 여기에 표시된 ACL에서 계속 작동합니다. 여기서 ICMP가 활성화되지만 보안 규칙에 따라 거부 또는 허용할 수 있습니다.

```
ip access-list extended REDIRECT
 deny icmp any any
deny udp any any eq bootps
 deny udp any any eq bootpc
 deny udp any any eq domain
deny ip any host 10.106.73.69
 permit tcp any any eq www
 permit tcp any any eq 443
```

주의: HTTPS를 활성화하면 확장성으로 인해 일부 높은 CPU 문제가 발생할 수 있습니다. Cisco 설계 팀에서 권장하지 않는 한 이 옵션을 활성화하지 마십시오.

3. 앵커에서 모빌리티를 구성합니다.

```
wireless mobility group member ip 10.105.135.244 public-ip 10.105.135.244 group surbg
```

참고: 3850 스위치에 외래 스위치로 동일한 를 구성한 경우 모빌리티 컨트롤러에서 스위치 피어 그룹을 정의하고 모빌리티 컨트롤러에서 스위치 피어 그룹을 정의해야 합니다. 그런 다음 3850 스위치에서 위의 CWA 컨피그레이션을 구성합니다.

4. 앵커의 컨피그레이션. 앵커에서는 ISE 컨피그레이션을 구성할 필요가 없습니다. WLAN 컨피그레이션만 있으면 됩니다.

```
wlan MA-MC 6 MA-MC
 aaa-override
 client vlan VLAN0012
 mac-filtering MACFILTER
 mobility anchor
nac
 nbsp;no security wpa
 no security wpa akm dot1x
 no security wpa wpa2
 no security wpa wpa2 ciphers aes
 session-timeout 1800
 no shutdown
```

5. 앵커에서 모빌리티를 구성합니다. 다른 WLC를 이 WLC의 모빌리티 멤버로 정의합니다.

```
wireless mobility group member ip 10.105.135.178 public-ip 10.105.135.178 group surbg
```

6. CLI로 리디렉션 ACL을 구성합니다. 이는 ISE가 게스트 포털 리디렉션을 위한 리디렉션 URL과 함께 AAA 재정의로 반환하는 url-redirect-acl입니다. 현재 통합 아키텍처에서 사용되는 직접 ACL입니다. 이는 'punt' ACL로, Unified Architecture에 일반적으로 사용하는 일종의 역방향 ACL입니다. DHCP, DHCP 서버, DNS, DNS 서버 및 ISE 서버에 대한 액세스를 차단해야 합니다. 필요에 따라 www, 443 및 8443만 허용합니다. 이 ISE 게스트 포털에서는 포트 8443을 사용하며 리디렉션은 여기에 표시된 ACL에서 계속 작동합니다. 여기서 ICMP가 활성화되지만 보안 규칙에 따라 거부 또는 허용할 수 있습니다.

```
ip access-list extended REDIRECT
 deny icmp any any
```

```
deny udp any any eq bootps
deny udp any any eq bootpc
deny udp any any eq domain
deny ip any host 10.106.73.69
permit tcp any any eq www
permit tcp any any eq 443
```

주의: HTTPS를 활성화하면 확장성으로 인해 일부 높은 CPU 문제가 발생할 수 있습니다. Cisco 설계 팀에서 권장하지 않는 한 이 옵션을 활성화하지 마십시오.

토폴로지 3 컨피그레이션 예

네트워크 다이어그램 및 설명은 토폴로지 3을 참조하십시오.

이는 2단계 프로세스이기도 합니다.

ISE의 컨피그레이션

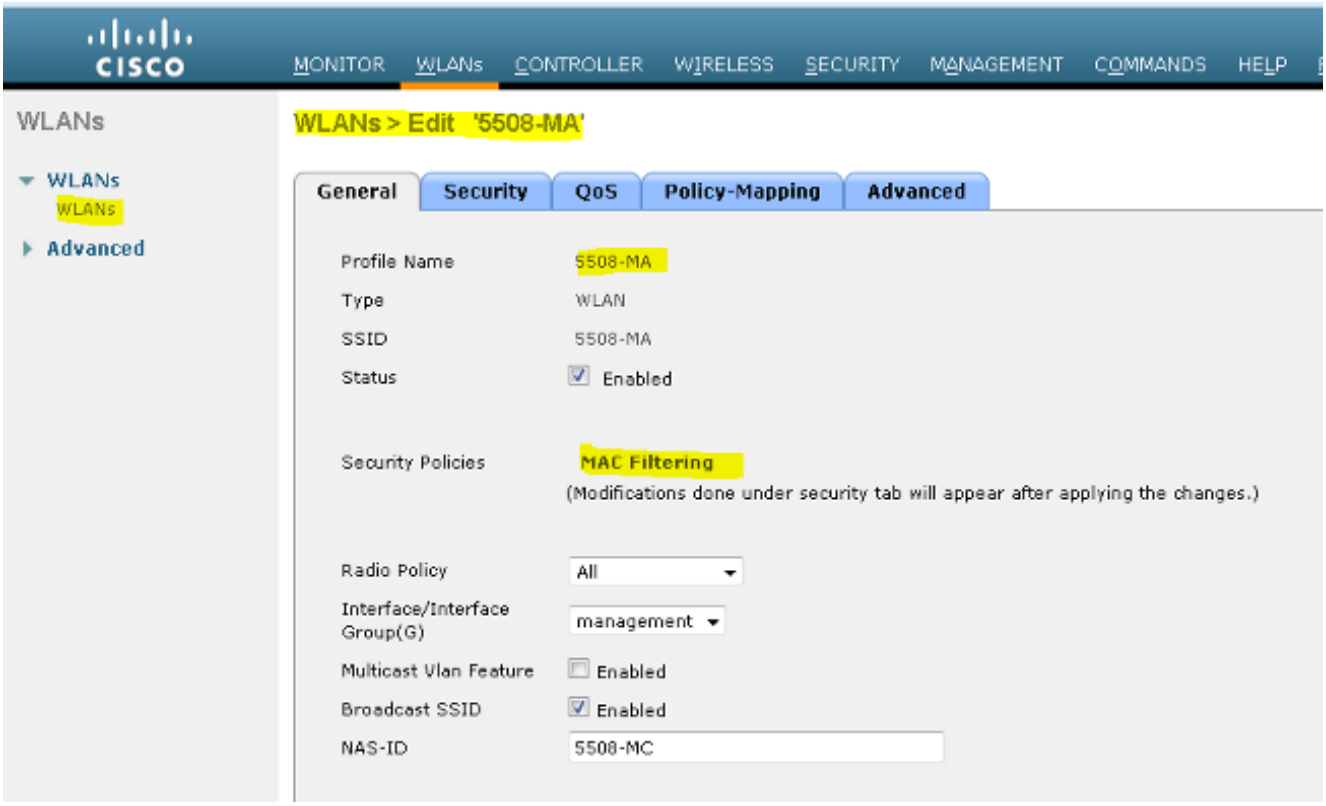
ISE의 컨피그레이션은 토폴로지 1 컨피그레이션과 동일합니다.

ISE에 Anchor Controller를 추가할 필요가 없습니다. ISE에 외부 WLC를 추가하고, 외부 WLC에서 RADIUS 서버를 정의하고, WLAN에 권한 부여 정책을 매핑하기만 하면 됩니다. 앵커에서는 MAC 필터링을 활성화하기만 하면 됩니다.

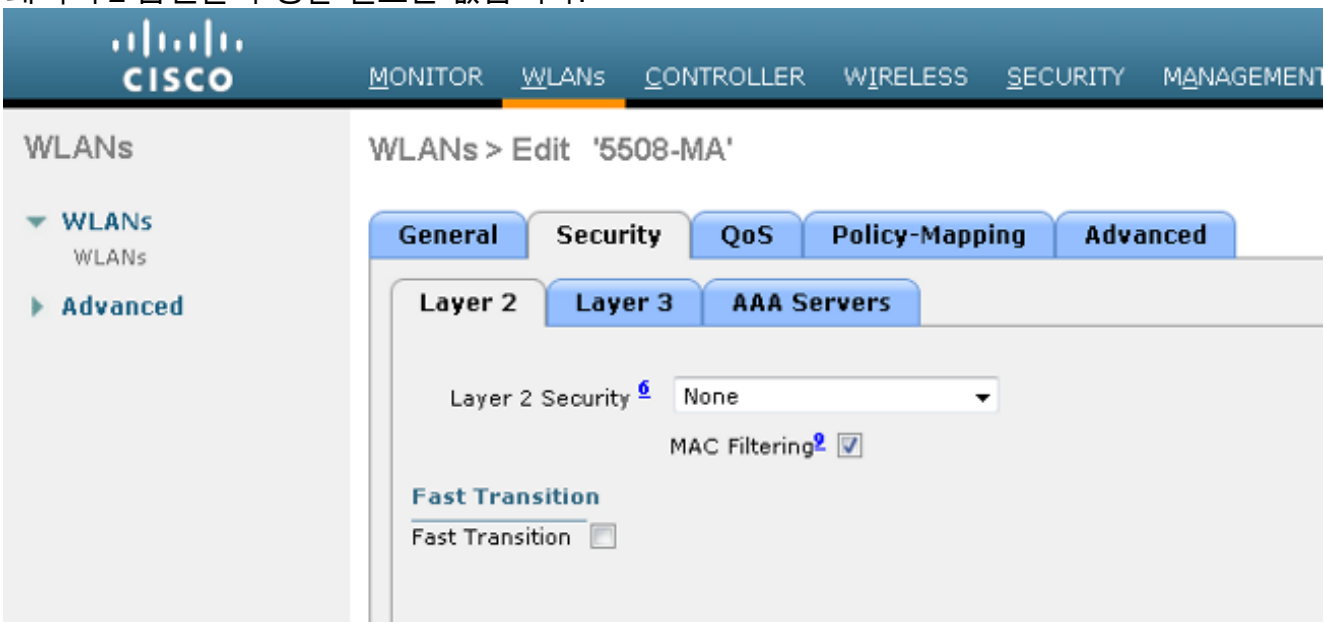
이 예에서는 앵커 역할을 하는 WLC 5508 및 외부 WLC 역할을 하는 WLC 5760이 있습니다. WLC 5508을 앵커 및 3850 스위치로 사용하고 모빌리티 에이전트인 외부 WLC를 다른 모빌리티 컨트롤러에 사용하려는 경우 동일한 컨피그레이션이 올바릅니다. 그러나 3850 스위치에서 라이센스를 가져오는 두 번째 모빌리티 컨트롤러에서 WLAN을 구성할 필요는 없습니다. 3850 스위치를 앵커 역할을 하는 5508 WLC로 가리키기만 하면 됩니다.

WLC의 컨피그레이션

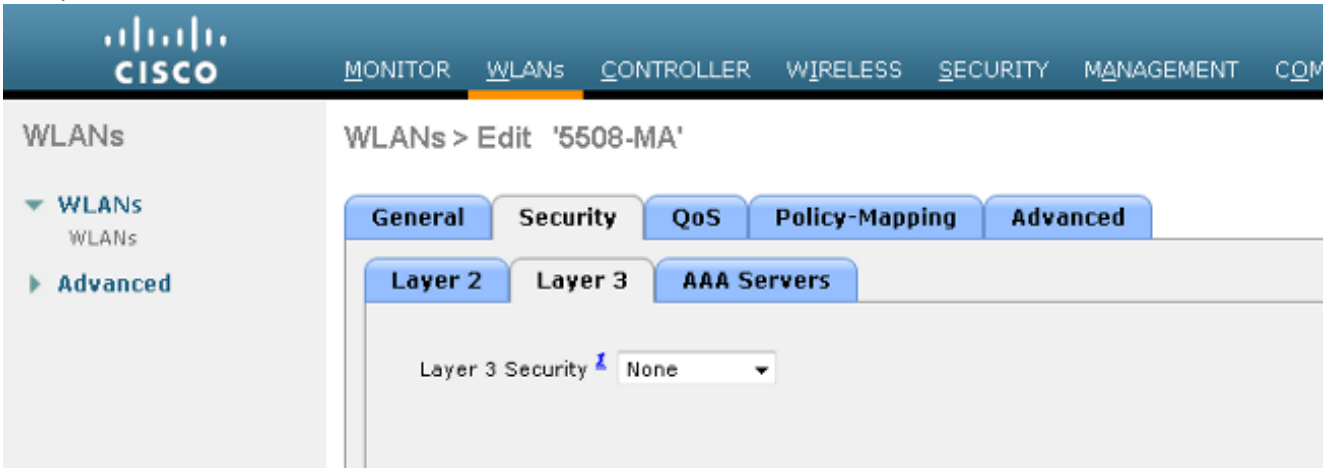
1. 외부 WLC에서 AAA에 대한 AAA Method(AAA 방법) 목록을 사용하여 ISE 서버를 구성하고 WLAN을 MAC 필터 권한 부여에 매핑합니다. 앵커에서는 필요하지 않습니다. **참고**: 앵커 및 외부 WLC와 MAC 필터링 모두에서 리디렉션 ACL을 구성합니다.
2. WLC 5508 GUI에서 WLANs(**WLANs) > New(새로 만들기)**를 선택하여 앵커 5508을 구성합니다. MAC 필터링을 활성화하려면 세부 정보를 입력합니다.



3. 레이어 2 옵션을 구성할 필요는 없습니다.

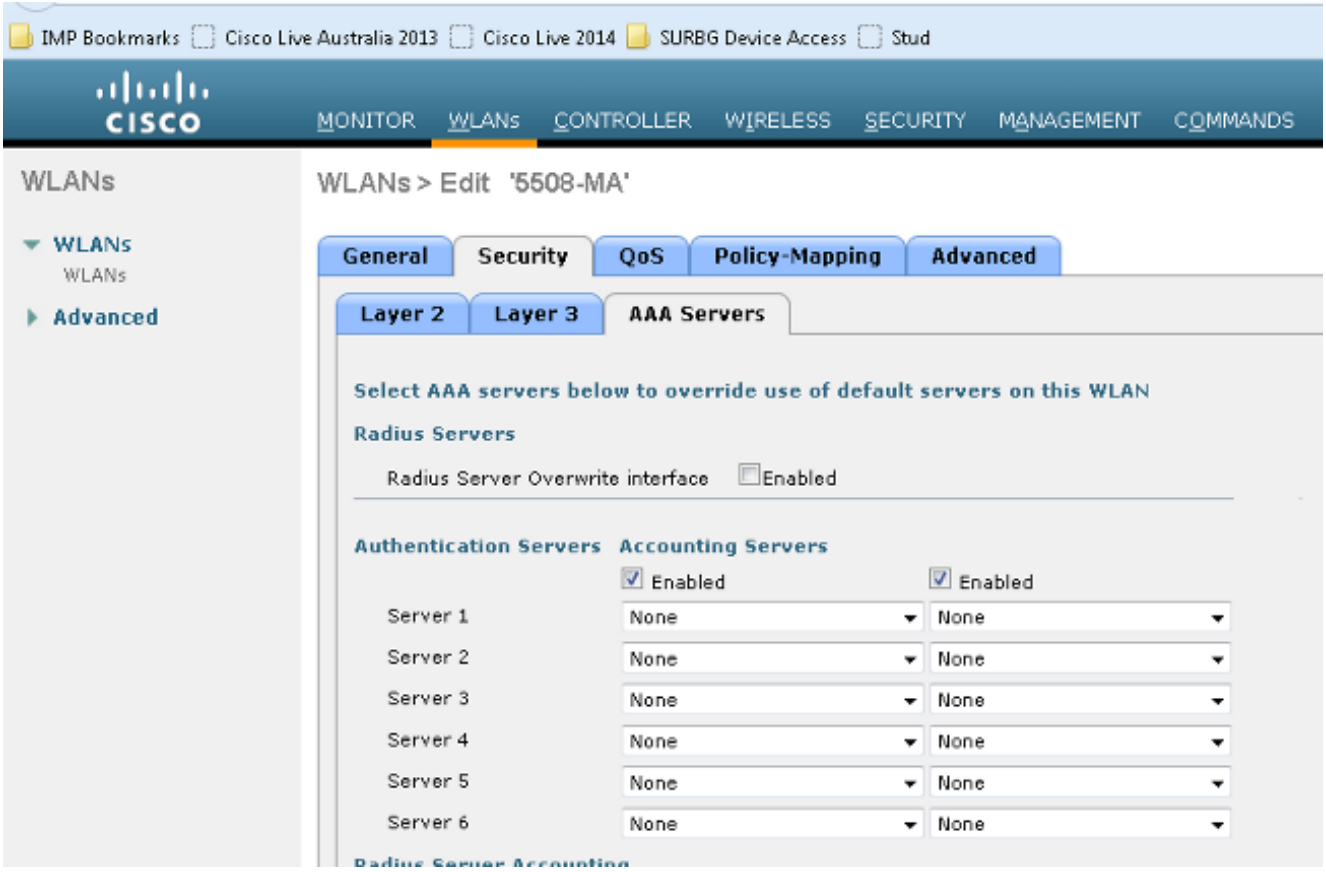


4. 레이어 3 옵션을 구성할 필요는 없습니다.

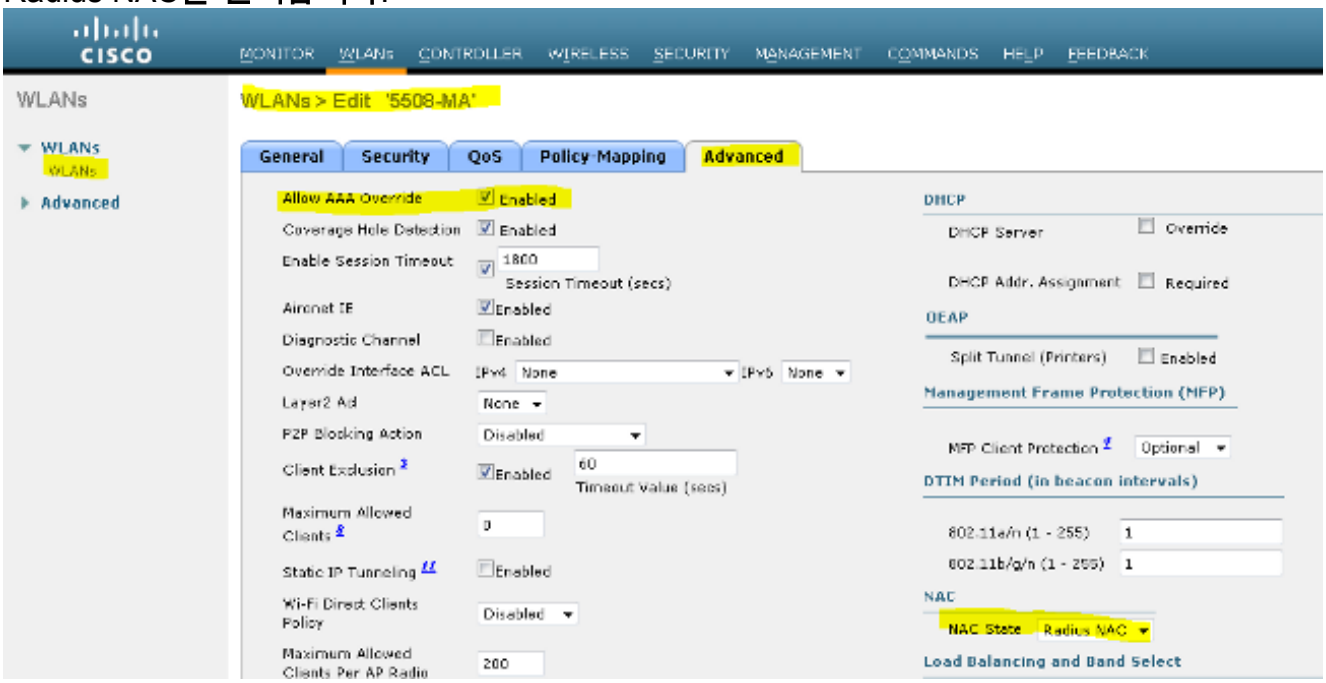


5. CoA를 외부 NGWC에서 처리하려면 Anchor AireOS WLC에서 AAA 서버를 비활성화해야 합

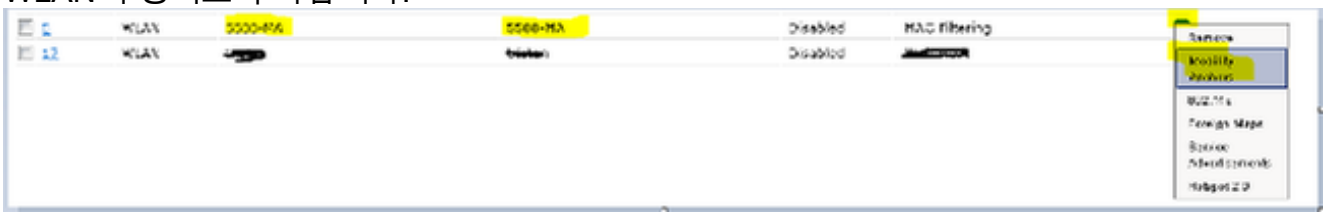
니다. AAA 서버는 Security(보안) > AAA > RADIUS > Authentication(인증)에 구성된 RADIUS 서버가 없는 경우에만 앵커 WLC에서 활성화할 수 있습니다.



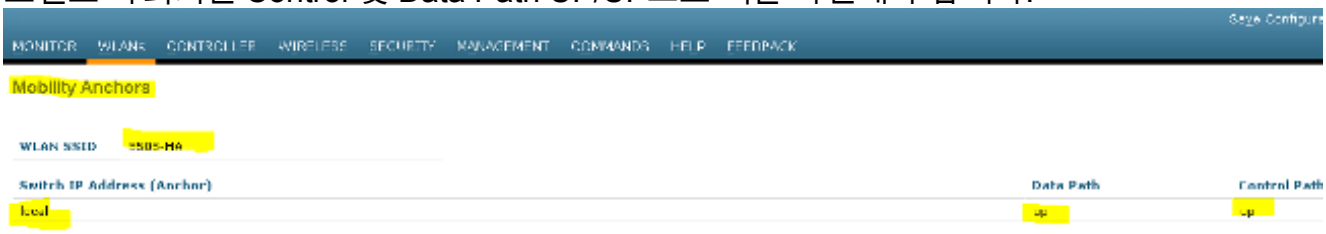
6. WLANs(**WLAN) > WLANs(WLAN) > Edit(편집) > Advanced(고급)를 선택합니다**. Allow **AAA Override(AAA 재정의 허용**) 확인란을 선택합니다. NAC State(NAC 상태) 드롭다운 목록에서 **Radius NAC를 선택합니다**.



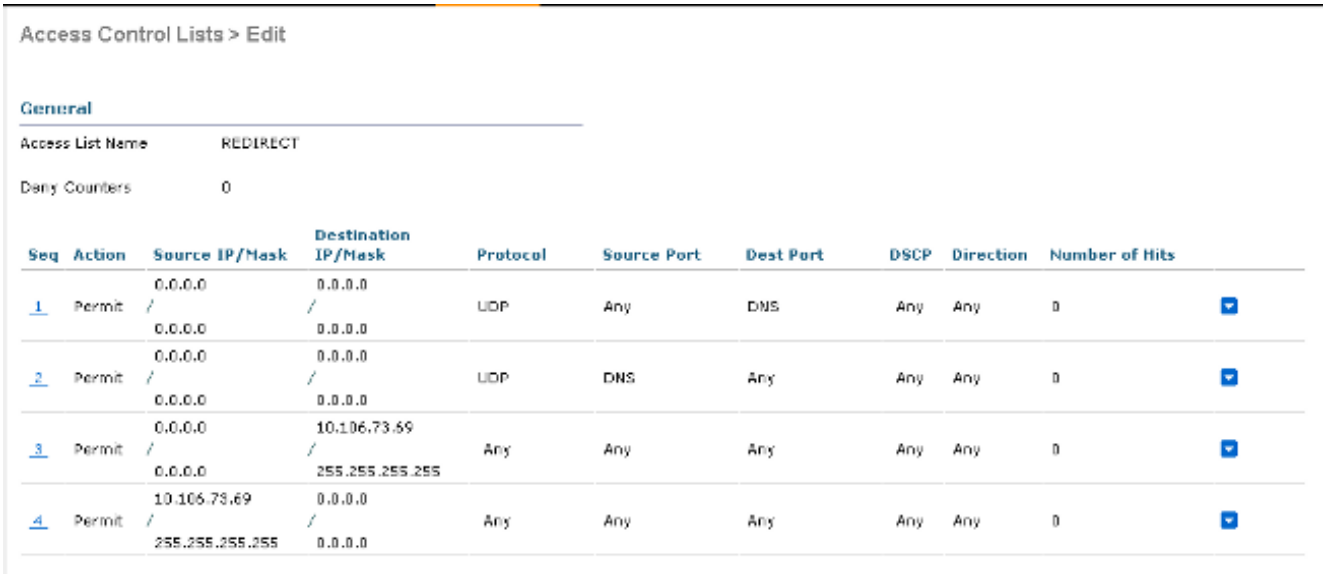
7. WLAN의 앵커로 추가합니다.



8. 로컬로 가리키면 Control 및 Data Path UP/UP으로 이를 확인해야 합니다.

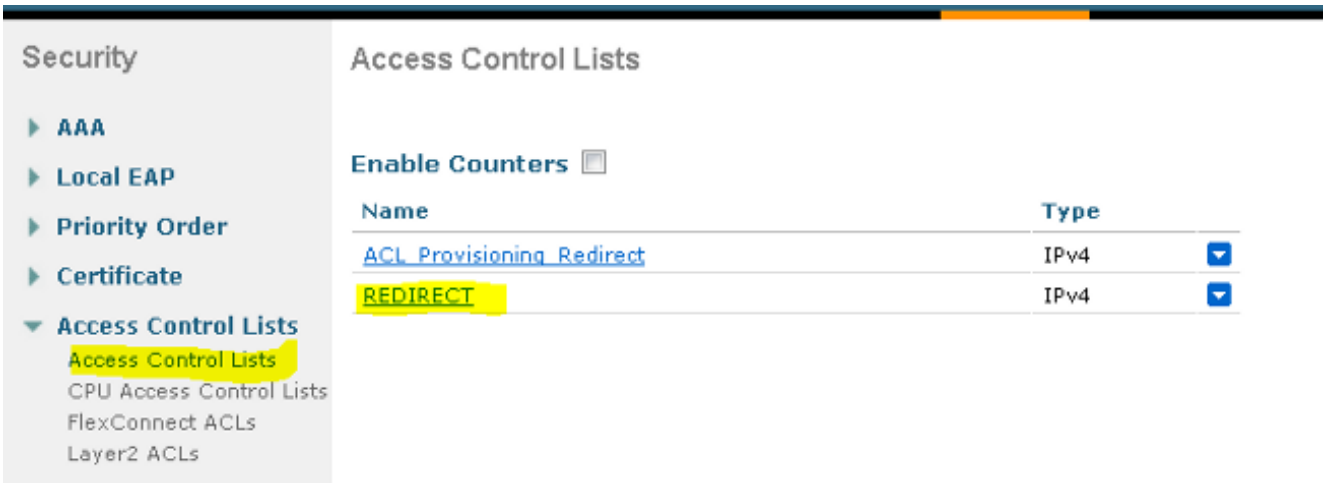


9. WLC에서 리디렉션 ACL을 생성합니다. 이는 DHCP 및 DNS를 거부합니다. HTTP/HTTP를 허용합니다.



이는 ACL이 생성된 후의 모습입니다

.



10. WLC 5760에서 ISE RADIUS 서버를 정의합니다.
11. CLI를 사용하여 RADIUS 서버, 서버 그룹 및 방법 목록을 구성합니다.

```
dot1x system-auth-control

radius server ISE
 address ipv4 10.106.73.69 auth-port 1645 acct-port 1646
 timeout 10
 retransmit 3
 key Cisco123


aaa group server radius ISE
 server name ISE
 deadtime 10

aaa authentication dot1x ISE group ISE
```

```
aaa authorization network ISE group ISE

aaa authorization network MACFILTER group ISE

aaa accounting identity ISE start-stop group ISE

!

aaa server radius dynamic-author
 client 10.106.73.69 server-key Cisco123
 auth-type any
```

12. CLI에서 WLAN을 구성합니다.

```
wlan 5508-MA 15 5508-MA
 aaa-override
 accounting-list ISE
 client vlan VLAN0012
 mac-filtering MACFILTER
 mobility anchor 10.105.135.151
 nac
 no security wpa
 no security wpa akm dot1x
 no security wpa wpa2
 no security wpa wpa2 ciphers aes
 security dot1x authentication-list ISE
 session-timeout 1800
 shutdown
```

13. 다른 WLC를 이 WLC의 모빌리티 멤버로 정의합니다.

```
wireless mobility group member ip 10.105.135.151public-ip 10.105.135.151 group Mobile-1
```

참고: WLC 3850에서 외래 스위치로 동일한 포트를 구성할 경우 모빌리티 컨트롤러에서 스위치 피어 그룹을 정의하는지, 모빌리티 컨트롤러에서 스위치 피어 그룹을 정의하는지 확인하십시오. 그런 다음 WLC 3850에서 이전 CWA 컨피그레이션을 구성합니다.

14. CLI로 리디렉션 ACL을 구성합니다. 이는 ISE가 게스트 포털 리디렉션을 위한 리디렉션 URL과 함께 AAA 재정의로 반환하는 url-redirect-acl입니다. 현재 통합 아키텍처에서 사용되는 직접 ACL입니다. 이는 'punt' ACL로, Unified Architecture에 일반적으로 사용하는 일종의 역방향 ACL입니다. DHCP, DHCP 서버, DNS, DNS 서버 및 ISE 서버에 대한 액세스를 차단해야 합니다. 필요에 따라 www, 443 및 8443만 허용합니다. 이 ISE 게스트 포털에서는 포트 8443을 사용하며 리디렉션은 여기에 표시된 ACL에서 계속 작동합니다. 여기서 ICMP가 활성화되지만 보안 규칙에 따라 거부 또는 허용할 수 있습니다.

```
ip access-list extended REDIRECT
 deny icmp any any
 deny udp any any eq bootps
 deny udp any any eq bootpc
 deny udp any any eq domain
 deny ip any host 10.106.73.69
 permit tcp any any eq www
 permit tcp any any eq 443
```

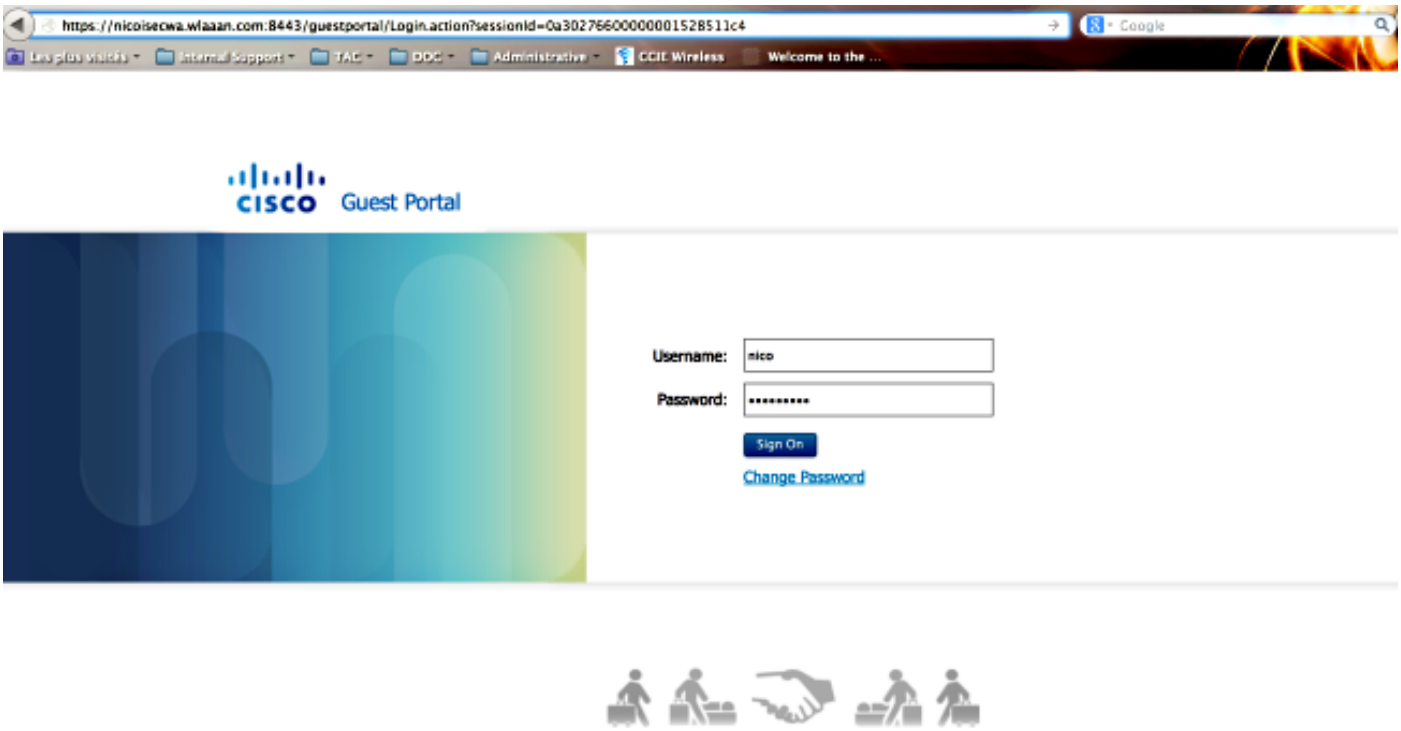
주의: HTTPS를 활성화하면 확장성으로 인해 일부 높은 CPU 문제가 발생할 수 있습니다. Cisco 설계 팀에서 권장하지 않는 한 이 옵션을 활성화하지 마십시오.

다음을 확인합니다.

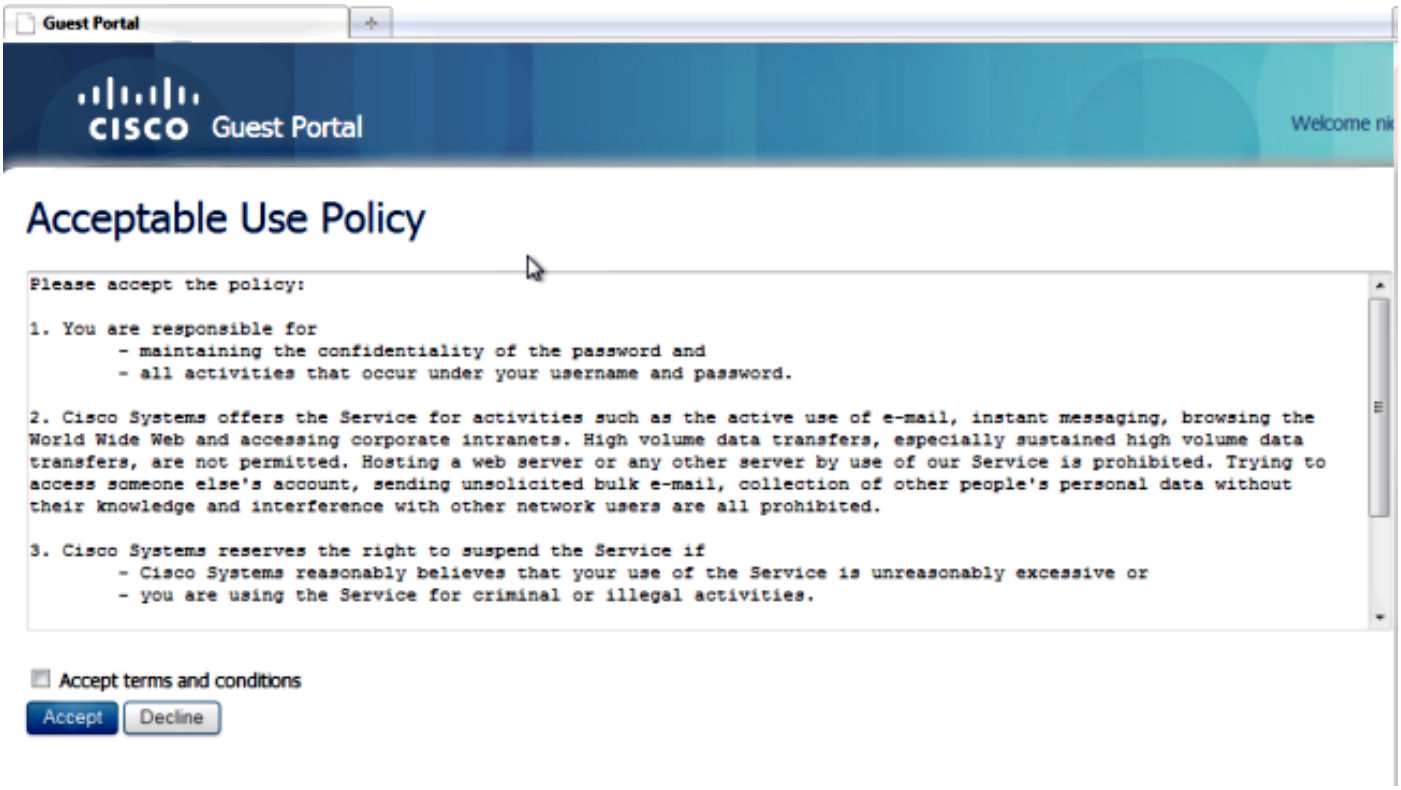
설정이 올바르게 작동하는지 확인하려면 이 섹션을 활용하십시오.

아웃풋 인터프리터 툴(등록 고객 전용)은 특정 **show** 명령을 지원합니다. **show** 명령 출력의 분석을 보려면 아웃풋 인터프리터 툴을 사용합니다.

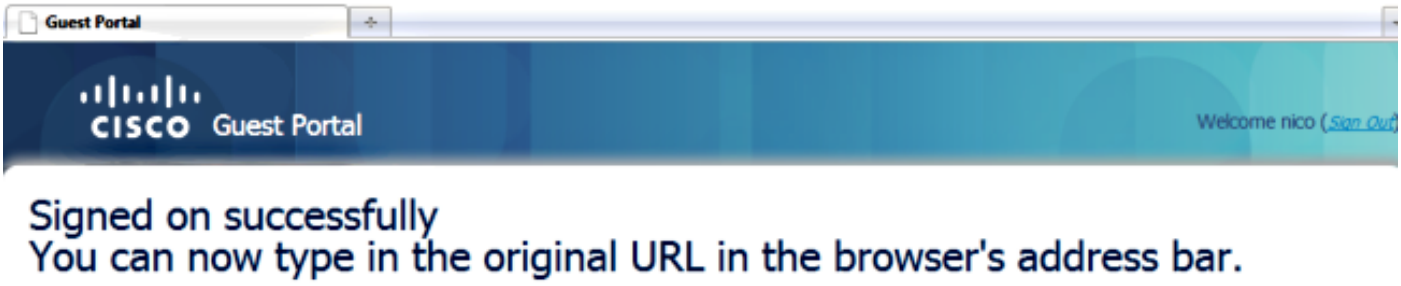
구성된 SSID에 클라이언트를 연결합니다. IP 주소를 수신하고 클라이언트가 웹 인증 필요 상태로 전환되면 브라우저를 엽니다. 포털에 클라이언트 자격 증명을 입력 합니다.



인증에 성공한 후 Accept terms **and conditions(약관 동의) 확인란**을 선택합니다. Accept를 **클릭합니다**.

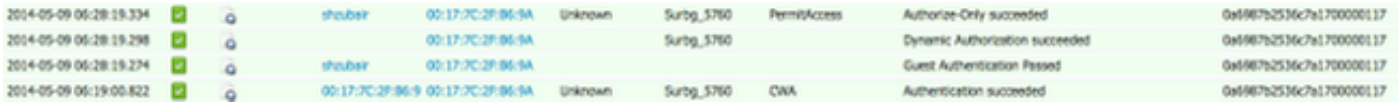


확인 메시지가 표시되고 이제 인터넷을 탐색할 수 있습니다.



You can now type in the original URL in the browser's address bar.

ISE에서 클라이언트 흐름은 다음과 같습니다.



문제 해결

이 섹션에서는 설정 문제 해결에 사용할 수 있는 정보를 제공합니다.

아웃풋 인터프리터 툴(등록 고객 전용)은 특정 **show** 명령을 지원합니다. **show** 명령 출력의 분석을 보려면 아웃풋 인터프리터 툴을 사용합니다.

> **참고**: debug 명령을 사용하기 전에 Debug 명령에 대한 중요 정보를 참조하십시오.

Converged Access WLC에서는 디버깅 대신 추적을 실행하는 것이 좋습니다. Aironet OS 5508 WLC에서 **debug client <client mac>** 및 debug **web-auth redirect enable mac <client mac>만** 입력하면 됩니다.

```
set trace group-wireless-client level debug
set trace group-wireless-secure level debug

set trace group-wireless-client filter mac 0017.7c2f.b69a
set trace group-wireless-secure filter mac 0017.7c2f.b69a
```

Cisco IOS-XE 및 Aironet OS의 일부 알려진 결함은 Cisco 버그 ID CSCun38344에 포함되어 있습니다.

다음은 추적에서 성공한 CWA 흐름의 모습입니다.

```
[05/09/14 13:13:15.951 IST 63d7 8151] 0017.7c2f.b69a Association received from mobile
on AP c8f9.f983.4260
[05/09/14 13:13:15.951 IST 63d8 8151] 0017.7c2f.b69a qos upstream policy is unknown
and downstream policy is unknown

[05/09/14 13:13:15.951 IST 63e0 8151] 0017.7c2f.b69a Applying site-specific IPv6
override for station  0017.7c2f.b69a  - vapId 15, site 'default-group', interface
```

'VLAN0012'
[05/09/14 13:13:15.951 IST 63e1 8151] 0017.7c2f.b69a Applying local bridging Interface Policy for station 0017.7c2f.b69a - vlan 12, interface 'VLAN0012'
[05/09/14 13:13:15.951 IST 63e2 8151] 0017.7c2f.b69a
 **** Inside applyLocalProfilingPolicyAction ****

[05/09/14 13:13:15.951 IST 63e3 8151] 0017.7c2f.b69a *** **Client State = START** instance = 1 instance Name POLICY_PROFILING_80211_ASSOC, OverrideEnable = 1 deviceTypeLen=0, deviceType=(null), userRoleLen=0, userRole=(null

[05/09/14 13:13:15.951 IST 63eb 8151] 0017.7c2f.b69a AAAS: Submitting mac filter request for user 00177c2fb69a, uniqueId=280 mlist=MACFILTER
[05/09/14 13:13:15.951 IST 63ec 8151] 0017.7c2f.b69a AAAS: auth request sent
05/09/14 13:13:15.951 IST 63ed 8151] 0017.7c2f.b69a apfProcessAssocReq (apf_80211.c:6149) Changing state for mobile 0017.7c2f.b69a on AP c8f9.f983.4260 from Idle to AAA Pending

[05/09/14 13:13:15.951 IST 63ee 8151] 0017.7c2f.b69a Reason code 0, Preset 4, AAA cause 1
[05/09/14 13:13:15.951 IST 63ef 8151] 0017.7c2f.b69a Scheduling deletion of Mobile Station: (callerId: 20) in 10 seconds
[05/09/14 13:13:15.951 IST 63f0 211] **Parsed CLID MAC Address = 0:23:124:47:182:154**
[05/09/14 13:13:15.951 IST 63f1 211] AAA SRV(00000118): process author req
[05/09/14 13:13:15.951 IST 63f2 211] **AAA SRV(00000118): Author method=SERVER_GROUP Zubair_ISE**
[05/09/14 13:13:16.015 IST 63f3 220] AAA SRV(00000118): protocol reply PASS for Authorization
[05/09/14 13:13:16.015 IST 63f4 220] AAA SRV(00000118): Return Authorization status=PASS
[05/09/14 13:13:16.015 IST 63f5 8151] 0017.7c2f.b69a AAAS: received response, cid=266
[05/09/14 13:13:16.015 IST 63f6 8151] 0017.7c2f.b69a AAAS: deleting context, cid=266
[05/09/14 13:13:16.015 IST 63f7 8151] 0017.7c2f.b69a Not comparing because the ACLs have not been sent yet.
[05/09/14 13:13:16.015 IST 63f8 8151] 0017.7c2f.b69a Final flag values are, epmSendAcl 1, epmSendAclDone 0
[05/09/14 13:13:16.015 IST 63f9 8151] 0017.7c2f.b69a
client incoming attribute size are 193
[05/09/14 13:13:16.015 IST 63fa 8151] 0017.7c2f.b69a AAAS: mac filter callback status=0 uniqueId=280
[05/09/14 13:13:16.015 IST 63fb 8151] 0017.7c2f.b69a AAA Override Url-Redirect 'https://10.106.73.69:8443/guestportal/gateway?sessionId=0a6987b2536c871300000118&action=cwa' set
[05/09/14 13:13:16.015 IST 63fc 8151] **0017.7c2f.b69a Redirect URL received for client from RADIUS. for redirection.**
[05/09/14 13:13:16.015 IST 63fd 8151] 0017.7c2f.b69a Setting AAA Override Url-Redirect-Acl 'REDIRECT'
[05/09/14 13:13:16.015 IST 63fe 8151] 0017.7c2f.b69a AAA Override Url-Redirect-Acl 'REDIRECT'
[05/09/14 13:13:16.015 IST 63ff 8151] 0017.7c2f.b69a Local Policy: At the start of apfApplyOverride2. Client State START

[05/09/14 13:13:16.015 IST 6400 8151] 0017.7c2f.b69a Applying new AAA override for station 0017.7c2f.b69a
[05/09/14 13:13:16.015 IST 6401 8151] 0017.7c2f.b69a Local Policy: Applying new AAA override for station
[05/09/14 13:13:16.015 IST 6402 8151] 0017.7c2f.b69a Override Values: source: 2, valid_bits: 0x0000, qosLevel: -1 dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout: -1
[05/09/14 13:13:16.015 IST 6403 8151] 0017.7c2f.b69a dataAvgC: -1, rTAvgC: -1, dataBurstC: -1 rTimeBurstC: -1, vlanIfName: , aclName:
[05/09/14 13:13:16.015 IST 6404 8151] 0017.7c2f.b69a Local Policy: Applying override policy
[05/09/14 13:13:16.015 IST 6405 8151] 0017.7c2f.b69a Clearing Dhcp state for station ---
[05/09/14 13:13:16.015 IST 6406 8151] 0017.7c2f.b69a Local Policy: Before Applying WLAN policy AccessVLAN = 12 and SessionTimeout is 1800 and apfMsTimeout is 1800

[05/09/14 13:13:16.015 IST 6407 8151] 0017.7c2f.b69a Local Policy:Setting
Interface name e VLAN0012

[05/09/14 13:13:16.015 IST 6408 8151] 0017.7c2f.b69a Local Policy:Setting local bridging VLAN name VLAN0012 and VLAN ID 12

[05/09/14 13:13:16.015 IST 6409 8151] 0017.7c2f.b69a Applying WLAN ACL
policies to client
[05/09/14 13:13:16.015 IST 640a 8151] 0017.7c2f.b69a No Interface ACL
used for Wireless client in WCM(NGWC)
[05/09/14 13:13:16.015 IST 640b 8151] 0017.7c2f.b69a apfApplyWlanPolicy:
Retaining the ACL recieved in AAA attributes 255 on mobile
[05/09/14 13:13:16.015 IST 640c 8151] 0017.7c2f.b69a Local Policy: After
Applying WLAN policy AccessVLAN = 12 and SessionTimeout is 1800 and
apfMsTimeout is 1800

[05/09/14 13:13:16.015 IST 641a 8151] 0017.7c2f.b69a WCDB_ADD: Platform
ID allocated successfully ID:259
[05/09/14 13:13:16.015 IST 641b 8151] 0017.7c2f.b69a WCDB_ADD: Adding
opt82 len 0
[05/09/14 13:13:16.015 IST 641c 8151] 0017.7c2f.b69a WCDB_ADD: ssid
5508-MA bssid c8f9.f983.4260 vlan 12 auth=ASSOCIATION(0)
wlan(ap-group/global) 15/15 client 0 assoc 1 mob=Unassoc(0) radio 0
m_vlan 12 ip 0.0.0.0 src 0x506c800000000f dst 0x0 cid 0x47ad4000000145
glob rsc id 259dhcpsrv 0.0.0
[05/09/14 13:13:16.015 IST 641d 8151] 0017.7c2f.b69a Change state to
AUTHCHECK (2) last state START (0)

[05/09/14 13:13:16.015 IST 641e 8151] 0017.7c2f.b69a Change state to L2AUTHCOMPLETE (4) last state AUTHCHECK (2)

[05/09/14 13:13:16.015 IST 641f 8151] 0017.7c2f.b69a WCDB_AUTH: Adding opt82 len 0
[05/09/14 13:13:16.015 IST 6420 8151] 0017.7c2f.b69a WCDB_LLM: NoRun Prev Mob 0,
Curr Mob 0 llmReq 1, return False
[05/09/14 13:13:16.015 IST 6421 207] [WCDB] ==Add event: type Regular Wireless client
(0017.7c2f.b69a) client id (0x47ad4000000145) client index (259) vlan (12)
auth_state (ASSOCIATION) mob_state (INIT)
[05/09/14 13:13:16.015 IST 6422 207] [WCDB] ===intf src/dst (0x506c800000000f)/(0x0)
radio_id (0) p2p_state (P2P_BLOCKING_DISABLE) switch/asic (1/0)
[05/09/14 13:13:16.015 IST 6423 8151] 0017.7c2f.b69a WCDB_CHANGE: auth=L2_AUTH(1)
vlan 12 radio 0 client_id 0x47ad4000000145 mobility=Unassoc(0) src_int
0x506c800000000f dst_int 0x0 ackflag 0 reassoc_client 0 llm_notif 0 ip 0.0.0.0
ip_learn_type 0
[05/09/14 13:13:16.015 IST 6424 8151] 0017.7c2f.b69a WCDB_CHANGE: In L2 auth
but l2ack waiting lfag not set,so set
[05/09/14 13:13:16.015 IST 6425 8151] 0017.7c2f.b69a Not Using WMM Compliance code
qosCap 00
[05/09/14 13:13:16.016 IST 6426 8151] 0017.7c2f.b69a **Change state to DHCP_REQD (7) last state L2AUTHCOMPLETE (4)**

[05/09/14 13:13:16.016 IST 6434 8151] 0017.7c2f.b69a Sending Assoc Response to
station on BSSID c8f9.f983.4260 (status 0) ApVapId 15 Slot 0
[05/09/14 13:13:16.016 IST 6435 8151] 0017.7c2f.b69a apfProcessRadiusAssocResp
(apf_80211.c:2316) Changing state for mobile 0017.7c2f.b69a on AP
c8f9.f983.4260 from Associated to Associated

[05/09/14 13:13:16.016 IST 6436 8151] 0017.7c2f.b69a 1XA: Session Push for
Non-dot1x wireless client
[05/09/14 13:13:16.016 IST 6437 8151] 0017.7c2f.b69a 1XA: Calling Auth Mgr
to Push wireless session for client 47ad4000000145 uid 280
[05/09/14 13:13:16.016 IST 6438 8151] 0017.7c2f.b69a Session Push for
wireless client

```
[05/09/14 13:13:16.016 IST 6439 8151] 0017.7c2f.b69a Session Manager Call
Client 47ad4000000145, uid 280, capwap id 506c800000000f,Flag 1 Audit-Session
ID 0a6987b2536c871300000118 policy name (null)

[05/09/14 13:13:16.016 IST 643a 22] ACCESS-CORE-SM-CLIENT-SPI-NOTF:
[0017.7c2f.b69a, Ca2] Session start request from Client[1] for
0017.7c2f.b69a (method: No method, method list: none, aaa id:
0x00000118) - session-push,  policy
[05/09/14 13:13:16.016 IST 643b 22] ACCESS-CORE-SM-CLIENT-SPI-NOTF:
[0017.7c2f.b69a, Ca2]  - client iif_id: 47AD4000000145, session ID:
0a6987b2536c871300000118 for 0017.7c2f.b69a
[05/09/14 13:13:16.016 IST 643c 243] ACCESS-CORE-SM-SYNC-NOTF:
[0017.7c2f.b69a, Ca2] Delay add/update sync of auth-domain for
0017.7c2f.b69a / 0xFE000110
[05/09/14 13:13:16.017 IST 643d 243] ACCESS-CORE-SM-CLIENT-DOT11-ERR:
[0017.7c2f.b69a, Ca2] Invalid client authorization notification: NO method
[05/09/14 13:13:16.017 IST 643e 243] ACCESS-CORE-SM-SYNC-NOTF:
[0017.7c2f.b69a, Ca2] Delay add/update sync of dc-profile-name for
0017.7c2f.b69a / 0xFE000110
[05/09/14 13:13:16.017 IST 643f 243] ACCESS-CORE-SM-SYNC-NOTF:
[0017.7c2f.b69a, Ca2] Delay add/update sync of dc-device-name for
0017.7c2f.b69a / 0xFE000110
[05/09/14 13:13:16.017 IST 6440 243] ACCESS-CORE-SM-SYNC-NOTF:
[0017.7c2f.b69a, Ca2] Delay add/update sync of
dc-device-class-tag for 0017.7c2f.b69a / 0xFE000110
[05/09/14 13:13:16.017 IST 6441 243] ACCESS-CORE-SM-SYNC-NOTF:
[0017.7c2f.b69a, Ca2] Delay add/update sync of dc-certainty-metric for
0017.7c2f.b69a / 0xFE000110
[05/09/14 13:13:16.017 IST 6442 243] ACCESS-CORE-SM-SYNC-NOTF:
[0017.7c2f.b69a, Ca2] Delay add/update sync of dc-opaque for
0017.7c2f.b69a / 0xFE000110
[05/09/14 13:13:16.017 IST 6443 243] ACCESS-CORE-SM-SYNC-NOTF:
[0017.7c2f.b69a, Ca2] Delay add/update sync of dc-protocol-map for
0017.7c2f.b69a / 0xFE000110
[05/09/14 13:13:16.017 IST 6444 22] [WCDB] wcdb_ffcp_add_cb: client (0017.7c2f.b69a)
client (0x47ad4000000145): FFCP operation (CREATE) return code (0)
[05/09/14 13:13:16.017 IST 6445 22] [WCDB] wcdb_send_add_notify_callback_event:
Notifying other features about client add
[05/09/14 13:13:16.017 IST 6446 22] [WCDB] wcdb_sisf_client_add_notify:
Notifying SISF of DEASSOC to DOWN any old entry for 0017.7c2f.b69a
[05/09/14 13:13:16.017 IST 6447 22] [WCDB] wcdb_sisf_client_add_notify:
Notifying SISF of new Association for 0017.7c2f.b69a
[05/09/14 13:13:16.017 IST 6448 8151] 0017.7c2f.b69a WCDB SPI response msg handler
client code 0 mob state 0
[05/09/14 13:13:16.017 IST 6449 8151] 0017.7c2f.b69a WcdbClientUpdate: L2 Auth ACK
from WCDB
[05/09/14 13:13:16.017 IST 644a 8151] 0017.7c2f.b69a WCDB_L2ACK: wcdbAckRecvdFlag
updated
[05/09/14 13:13:16.017 IST 644b 8151] 0017.7c2f.b69a WCDB_AUTH: Adding opt82 len 0
[05/09/14 13:13:16.017 IST 644c 8151] 0017.7c2f.b69a WCDB_CHANGE: Suppressing SPI
(Mobility state not known) pemstate 7 state LEARN_IP(2) vlan 12 client_id
0x47ad4000000145 mob=Unassoc(0) ackflag 2 dropd 1
[05/09/14 13:13:18.796 IST 644d 8151] 0017.7c2f.b69a Local Policy:
apf_ms_radius_override.c apfMsSumOverride 447  Returning fail from apfMsSumOverride
[05/09/14 13:13:18.802 IST 644e 8151] 0017.7c2f.b69a Applying post-handoff policy
for station  0017.7c2f.b69a  - valid mask 0x0

[05/09/14 13:13:18.802 IST 644f 8151] 0017.7c2f.b69a     QOS Level: -1, DSCP: -1,
dot1p: -1, Data Avg: -1, realtime Avg: -1, Data Burst -1, Realtime Burst -1
 --More--

[05/09/14 13:13:18.802 IST 6450 8151] 0017.7c2f.b69a     Session: -1,
User session: -1, User elapsed -1
   Interface: N/A ACL: N/A Qos Pol Down   Qos Pol Up
```

[05/09/14 13:13:18.802 IST 6451 8151] 0017.7c2f.b69a Local Policy: At the start of apfApplyOverride2. Client State DHCP_REQD

[05/09/14 13:13:18.802 IST 6452 8151] 0017.7c2f.b69a Applying new AAA override for station 0017.7c2f.b69a
[05/09/14 13:13:18.802 IST 6453 8151] 0017.7c2f.b69a Local Policy: Applying new AAA override for station
[05/09/14 13:13:18.802 IST 6454 8151] 0017.7c2f.b69a Override Values: source: 16, valid_bits: 0x0000, qosLevel: -1 dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout: -1
[05/09/14 13:13:18.802 IST 6455 8151] 0017.7c2f.b69a dataAvgC: -1, rTAvgC: -1, dataBurstC: -1 rTimeBurstC: -1, vlanIfName: , aclName:
[05/09/14 13:13:18.802 IST 6456 8151] 0017.7c2f.b69a Local Policy: Applying override policy
[05/09/14 13:13:18.802 IST 6457 8151] 0017.7c2f.b69a Clearing Dhcp state for station ---
[05/09/14 13:13:18.802 IST 6458 8151] 0017.7c2f.b69a Local Policy: Before Applying WLAN policy AccessVLAN = 12 and SessionTimeout is 1800 and apfMsTimeout is 1800

[05/09/14 13:13:18.802 IST 6459 8151] 0017.7c2f.b69a Local Policy:Setting Interface name e VLAN0012

[05/09/14 13:13:18.802 IST 645a 8151] 0017.7c2f.b69a Local Policy:Setting local bridging VLAN name VLAN0012 and VLAN ID 12

[05/09/14 13:13:18.802 IST 645b 8151] 0017.7c2f.b69a Applying WLAN ACL policies to client
[05/09/14 13:13:18.802 IST 645c 8151] 0017.7c2f.b69a No Interface ACL used for Wireless client in WCM(NGWC)
[05/09/14 13:13:18.802 IST 645d 8151] 0017.7c2f.b69a apfApplyWlanPolicy: Retaining the ACL recieved in AAA attributes 255 on mobile
[05/09/14 13:13:18.802 IST 645e 8151] 0017.7c2f.b69a Local Policy: After Applying WLAN policy AccessVLAN = 12 and SessionTimeout is 1800 and apfMsTimeout is 1800

[05/09/14 13:13:18.802 IST 645f 8151] 0017.7c2f.b69a Local Policy: After Applying Site Override policy AccessVLAN = 12 and SessionTimeout is 1800 and apfMsTimeout is 1800

[05/09/14 13:13:18.802 IST 6460 8151] 0017.7c2f.b69a Inserting AAA Override struct for mobile MAC: 0017.7c2f.b69a , source 16

[05/09/14 13:13:18.802 IST 6461 8151] 0017.7c2f.b69a Inserting new RADIUS override into chain for station 0017.7c2f.b69a
[05/09/14 13:13:18.802 IST 6462 8151] 0017.7c2f.b69a Override Values: source: 16, valid_bits: 0x0000, qosLevel: -1 dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout: -1
[05/09/14 13:13:18.802 IST 6463 8151] 0017.7c2f.b69a dataAvgC: -1, rTAvgC: -1, dataBurstC: -1 rTimeBurstC: -1, vlanIfName: , aclName:
[05/09/14 13:13:18.802 IST 6464 8151] 0017.7c2f.b69a Local Policy: After ovr check continuation
[05/09/14 13:13:18.802 IST 6465 8151] 0017.7c2f.b69a Local Policy: apf_ms_radius_override.c apfMsSumOverride 447 Returning fail from apfMsSumOverride
[05/09/14 13:13:18.802 IST 6466 8151] 0017.7c2f.b69a Local Policy: Calling applyLocalProfilingPolicyAction from Override2

[05/09/14 13:13:18.802 IST 6467 8151] 0017.7c2f.b69a
 **** Inside applyLocalProfilingPolicyAction ****

[05/09/14 13:13:18.802 IST 6468 8151] 0017.7c2f.b69a *** Client State = DHCP_REQD instance = 2 instance Name POLICY_PROFILING_L2_AUTH, OverrideEnable = 1 deviceTypeLen=0, deviceType=(null), userRoleLen=0,

```
userRole=(null)

[05/09/14 13:13:18.802 IST 6469 8151] 0017.7c2f.b69a     Local Profiling Values :
isValidVlan = 0, vlan = 0, isVlanRecdInDelete = 0, isValidSessionTimeout = 0,
 sessionTimeout=0, isSessionTORecdInDelete = 0  ProtocolMap = 0 ,applyPolicyAtRun= 0
[05/09/14 13:13:18.802 IST 646a 8151] 0017.7c2f.b69a          ipv4ACL = [],
ipv6ACL = [], inQoS = [unknown], outQoS = [unknown]
[05/09/14 13:13:18.802 IST 646b 8151] 0017.7c2f.b69a Local Policy: At the End
AccessVLAN = 12 and SessionTimeout  is 1800 and apfMsTimeout is 1800

[05/09/14 13:13:18.802 IST 646c 8151] 0017.7c2f.b69a apfMsRunStateInc
[05/09/14 13:13:18.802 IST 646d 8151] 0017.7c2f.b69a Session Update for Non-dot1x client

[05/09/14 13:13:18.802 IST 646e 8151] 0017.7c2f.b69a 1XA: Session Push for Non-dot1x
wireless client
[05/09/14 13:13:18.802 IST 646f 8151] 0017.7c2f.b69a 1XA: Calling Auth Mgr to Push
wireless session for client  47ad4000000145 uid 280
 --More--
[05/09/14 13:13:18.802 IST 6470 8151] 0017.7c2f.b69a Session Update for Pushed Sessions

[05/09/14 13:13:18.802 IST 6471 8151] 0017.7c2f.b69a Session Manager Call Client
47ad4000000145, uid 280, capwap id 506c800000000f,Flag 0 Audit-Session ID
0a6987b2536c871300000118 policy name (null)

[05/09/14 13:13:18.802 IST 6472 8151] 0017.7c2f.b69a Change state to RUN (20) last
state DHCP_REQD (7)

[05/09/14 13:13:18.802 IST 6473 8151] 0017.7c2f.b69a WCDB_AUTH: Adding opt82 len 0
[05/09/14 13:13:18.802 IST 6474 8151] 0017.7c2f.b69a WCDB_LLM: prev Mob state 0 curr
Mob State 3 llReq flag 1
[05/09/14 13:13:18.802 IST 6475 8151] 0017.7c2f.b69a WCDB_LLM: prev Mob state 0
currMob State 3 afd action 1
[05/09/14 13:13:18.802 IST 6476 8151] 0017.7c2f.b69a WCDB_LLM: pl handle 259 vlan_id
12 auth RUN(4) mobility 3 client_id 0x47ad4000000145 src_interface 0x506c800000000f
dst_interface 0x75e18000000143 client_type 0 p2p_type 1 bssid c8f9.f983.4260 radio_id
0 wgbid 0000.0000.0000
[05/09/14 13:13:18.802 IST 6477 8151] 0017.7c2f.b69a WCDB_CHANGE: auth=RUN(4) vlan
12 radio 0 client_id 0x47ad4000000145 mobility=ExpForeign(3) src_int 0x506c800000000f
dst_int 0x75e18000000143 ackflag 2 reassoc_client 0 llm_notif 1 ip  0.0.0.0
ip_learn_type 0
[05/09/14 13:13:18.802 IST 6478 22] ACCESS-CORE-SM-CLIENT-SPI-NOTF:
[0017.7c2f.b69a, Ca2] Session update from Client[1] for 0017.7c2f.b69a,
ID list 0x00000000, policy
[05/09/14 13:13:18.802 IST 6479 8151] 0017.7c2f.b69a WCDB_AUTH: Adding opt82 len 0
[05/09/14 13:13:18.802 IST 647a 8151] 0017.7c2f.b69a WCDB_LLM: prev Mob state 3
curr Mob State 3 llReq flag 0
[05/09/14 13:13:18.802 IST 647b 8151] 0017.7c2f.b69a WCDB_CHANGE: auth=RUN(4)
vlan 12 radio 0 client_id 0x47ad4000000145 mobility=ExpForeign(3) src_int
0x506c800000000f dst_int 0x75e18000000143 ackflag 2 reassoc_client 0 llm_notif 0
ip  0.0.0.0 ip_learn_type 0
[05/09/14 13:13:18.802 IST 647c 8151] 0017.7c2f.b69a AAAS: creating accounting start
record using method list Zubair_ISE, passthroughMode 1
[05/09/14 13:13:18.802 IST 647d 8151] 0017.7c2f.b69a AAAS: initialised accounting
start request, uid=280 passthrough=1
[05/09/14 13:13:18.802 IST 647e 8151] 0017.7c2f.b69a AAAS: accounting request sent
[05/09/14 13:13:18.803 IST 647f 207] [WCDB] ==Update event: client (0017.7c2f.b69a)
client id:(0x47ad4000000145) vlan (12->12) global_wlan (15->15) auth_state
(L2_AUTH_DONE->RUN) mob_st<truncated>
[05/09/14 13:13:18.803 IST 6480 207] [WCDB] ===intf src/dst
(0x506c800000000f->0x506c800000000f)/(0x0->0x75e18000000143)
radio/bssid (0->0)/(c8f9.f983.4260->c8f9.f983.4260) llm_notify (true) addr v4/v6
(<truncated>
[05/09/14 13:13:18.803 IST 6481 207] [WCDB] Foreign client add. Final llm
notified = false
```

```
[05/09/14 13:13:18.803 IST 6482 207] [WCDB] wcdb_client_mcast_update_notify:
No mcast action reqd
[05/09/14 13:13:18.803 IST 6483 207] [WCDB] wcdb_ffcp_wcdb_client_update_notify
client (0017.7c2f.b69a) id 0x47ad4000000145 ffcp update with flags=0x0
[05/09/14 13:13:18.803 IST 6484 207] [WCDB] wcdb_client_state_change_notify:
update flags = 0x3
[05/09/14 13:13:18.803 IST 6485 8151] 0017.7c2f.b69a aaa attribute list length is 79
[05/09/14 13:13:18.803 IST 6486 207] ACCESS-CORE-SM-CLIENT-DOT11-NOTF: [0017.7c2f.b69a]
WCDB RUN notification for 0017.7c2f.b69a
[05/09/14 13:13:18.803 IST 6487 8151] 0017.7c2f.b69a Sending SPI
spi_epm_epm_session_create successfull
[05/09/14 13:13:18.803 IST 6488 8151] 0017.7c2f.b69a 0.0.0.0, auth_state 20
mmRole ExpForeign !!!
[05/09/14 13:13:18.803 IST 6489 8151] 0017.7c2f.b69a 0.0.0.0, auth_state 20 mmRole
ExpForeign, updating wcdb not needed
[05/09/14 13:13:18.803 IST 648a 8151] 0017.7c2f.b69a Tclas Plumb needed: 0
[05/09/14 13:13:18.803 IST 648b 207] [WCDB] wcdb_sisf_client_update_notify:
Notifying SISF to remove assoc in Foreign
[05/09/14 13:13:18.803 IST 648c 207] [WCDB] ==Update event: client (0017.7c2f.b69a)
client id:(0x47ad4000000145) vlan (12->12) global_wlan (15->15) auth_state (RUN->RUN)
mob_st<truncated>
[05/09/14 13:13:18.803 IST 648d 207] [WCDB] ===intf src/dst
(0x506c800000000f->0x506c800000000f)/(0x75e18000000143->0x75e18000000143)
radio/bssid (0->0)/(c8f9.f983.4260->c8f9.f983.4260) llm_notify (false)
addr v4/v6 (<truncated>
[05/09/14 13:13:18.803 IST 648e 207] [WCDB] wcdb_client_mcast_update_notify:
No mcast action reqd
[05/09/14 13:13:18.803 IST 648f 207] [WCDB] wcdb_ffcp_wcdb_client_update_notify
client (0017.7c2f.b69a) id 0x47ad4000000145 ffcp update with flags=0x0
[05/09/14 13:13:18.803 IST 6490 207] [WCDB] wcdb_client_state_change_notify:
update flags = 0x2
[05/09/14 13:13:18.803 IST 6491 207] ACCESS-CORE-SM-CLIENT-DOT11-NOTF:
[0017.7c2f.b69a] WCDB RUN notification for 0017.7c2f.b69a
[05/09/14 13:13:18.803 IST 6492 207] [WCDB] wcdb_sisf_client_update_notify:
Notifying SISF to remove assoc in Foreign
[05/09/14 13:13:18.803 IST 6493 386] [WCDB] wcdb_ffcp_cb: client (0017.7c2f.b69a)
client (0x47ad4000000145): FFCP operation (UPDATE) return code (0)
[05/09/14 13:13:18.803 IST 6494 386] [WCDB] wcdb_ffcp_cb: client (0017.7c2f.b69a)
client (0x47ad4000000145): FFCP operation (UPDATE) return code (0)
[05/09/14 13:13:18.803 IST 6495 243] ACCESS-CORE-SM-SYNC-NOTF: [0017.7c2f.b69a, Ca2]
Delay add/update sync of iif-id for 0017.7c2f.b69a / 0xFE000110
[05/09/14 13:13:18.803 IST 6496 243] ACCESS-CORE-SM-SYNC-NOTF: [0017.7c2f.b69a, Ca2]
Delay add/update sync of audit-session-id for 0017.7c2f.b69a / 0xFE000110
[05/09/14 13:13:18.803 IST 6497 8151] 0017.7c2f.b69a Received session_create_response
for client handle 20175213735969093
[05/09/14 13:13:18.803 IST 6498 8151] 0017.7c2f.b69a Received session_create_response
with EPM session handle 4261413136
[05/09/14 13:13:18.803 IST 6499 8151] 0017.7c2f.b69a Splash Page redirect client
or posture client
 --More--
[05/09/14 13:13:18.803 IST 649a 8151] 0017.7c2f.b69a REDIRECT ACL present in the
attribute list
[05/09/14 13:13:18.803 IST 649b 8151] 0017.7c2f.b69a Setting AAA Override
Url-Redirect-Acl 'REDIRECT'
[05/09/14 13:13:18.803 IST 649c 8151] 0017.7c2f.b69a AAA Override Url-Redirect-Acl
'REDIRECT'
[05/09/14 13:13:18.803 IST 649d 8151] 0017.7c2f.b69a AAA Override Url-Redirect
'https://10.106.73.69:8443/guestportal/gateway?sessionId=0a6987b2536c871300000118&action=cwa'
set
[05/09/14 13:13:18.803 IST 649e 8151] 0017.7c2f.b69a  Wireless Client mobility role
is not ExportAnchor/Local. Hence we are not sending request to EPM
[05/09/14 13:13:20.445 IST 649f 8151] 0017.7c2f.b69a WCDB_IP_UPDATE: new ipv4 0.0.0.0
ip_learn_type 0 deleted ipv4 0.0.0.0
[05/09/14 13:13:20.446 IST 64a0 207] [WCDB] wcdb_foreign_client_ip_addr_update:
```

Foreign client (0017.7c2f.b69a) ip addr update received.
[05/09/14 13:13:20.446 IST 64a1 207] [WCDB] SISF Update: IPV6 Addr[0] :
fe80::6c1a:b253:d711:c7f
[05/09/14 13:13:20.446 IST 64a2 207] [WCDB] SISF Update : Binding delete status
for V6: = 0
[05/09/14 13:13:20.446 IST 64a3 207] [WCDB] wcdb_sisf_client_update_notify:
Notifying SISF to remove assoc in Foreign
[05/09/14 13:13:20.448 IST 64a4 8151] 0017.7c2f.b69a MS got the IP,
resetting the Reassociation Count 0 for client
[05/09/14 13:13:20.448 IST 64a5 8151] 0017.7c2f.b69a AAAS: creating accounting interim
record using method list Zubair_ISE, passthroughMode 1
[05/09/14 13:13:20.449 IST 64a6 8151] 0017.7c2f.b69a AAAS: initialised accounting
interim request, uid=280 passthrough=1
[05/09/14 13:13:20.449 IST 64a7 8151] 0017.7c2f.b69a AAAS: accounting request sent
[05/09/14 13:13:20.449 IST 64a8 8151] 0017.7c2f.b69a Guest User() assigned IP Address
(10.105.135.190)
[05/09/14 13:13:20.449 IST 64a9 8151] 0017.7c2f.b69a Assigning Address 10.105.135.190
to mobile
[05/09/14 13:13:20.449 IST 64aa 8151] 0017.7c2f.b69a WCDB_IP_UPDATE: new ipv4
10.105.135.190 ip_learn_type DHCP deleted ipv4 0.0.0.0
[05/09/14 13:13:20.449 IST 64ab 8151] 0017.7c2f.b69a AAAS: creating accounting
interim record using method list Zubair_ISE, passthroughMode 1
[05/09/14 13:13:20.449 IST 64ac 8151] 0017.7c2f.b69a AAAS: initialised accounting
interim request, uid=280 **passthrough=1**
[05/09/14 13:13:20.449 IST 64ad 8151] 0017.7c2f.b69a AAAS: accounting request sent
[05/09/14 13:13:20.449 IST 64ae 8151] 0017.7c2f.b69a 10.105.135.190, auth_state 20
mmRole ExpForeign !!!
[05/09/14 13:13:20.449 IST 64af 207] [WCDB] wcdb_foreign_client_ip_addr_update: Foreign
client (0017.7c2f.b69a) ip addr update received.
[05/09/14 13:13:20.449 IST 64b0 8151] 0017.7c2f.b69a 10.105.135.190, auth_state 20
mmRole ExpForeign, updating wcdb not needed
[05/09/14 13:13:20.449 IST 64b1 8151] 0017.7c2f.b69a Tclas Plumb needed: 0
[05/09/14 13:13:20.449 IST 64b2 207] [WCDB] SISF Update: IPV6 Addr[0] :
fe80::6c1a:b253:d711:c7f
[05/09/14 13:13:20.449 IST 64b3 207] [WCDB] SISF Update : Binding delete status for V6: = 0
[05/09/14 13:13:20.449 IST 64b4 207] [WCDB] wcdb_sisf_client_update_notify: Notifying SISF
to remove assoc in Foreign
[05/09/14 13:13:20.449 IST 64b5 243] ACCESS-CORE-SM-SYNC-NOTF: [0017.7c2f.b69a, Ca2] Delay
add/update sync of addr for 0017.7c2f.b69a / 0xFE000110
[05/09/14 13:13:49.429 IST 64b6 253] ACCESS-CORE-SM-CLIENT-SPI-NOTF: [0017.7c2f.b69a, Ca2]
Session authz update requested cmd 5, mac 0017.7c2f.b69a, attr-list 0x0 for Client[1]
[05/09/14 13:13:49.430 IST 64b7 253] ACCESS-CORE-SM-CLIENT-SPI-NOTF: [0017.7c2f.b69a, Ca2]
Session authz update request sent to Client[1]
[05/09/14 13:13:49.430 IST 64b8 8151] 0017.7c2f.b69a 1XA: Processing update request from
dot1x. COA type 5
[05/09/14 13:13:49.430 IST 64b9 8151] 0017.7c2f.b69a AAAS: authorization init, uid=280,
context=268
[05/09/14 13:13:49.430 IST 64ba 8151] 0017.7c2f.b69a AAAS: initialised auth request,
uinque id=280, context id = 268, context reqHandle 0xfefc172c
[05/09/14 13:13:49.430 IST 64bb 8151] 0017.7c2f.b69a AAAS: Submitting mac filter request
for user 00177c2fb69a, uniqueId=280 mlist=MACFILTER
[05/09/14 13:13:49.430 IST 64bc 8151] 0017.7c2f.b69a AAAS: auth request sent
[05/09/14 13:13:49.430 IST 64bd 8151] 0017.7c2f.b69a processing COA type 5
 was successful
[05/09/14 13:13:49.430 IST 64be 8151] 0017.7c2f.b69a processing COA type 5
 was successful
[05/09/14 13:13:49.430 IST 64bf 22] ACCESS-CORE-SM-CLIENT-SPI-NOTF: [0017.7c2f.b69a, Ca2]
Session authz update response received for Client[1]
[05/09/14 13:13:49.430 IST 64c0 211] Parsed CLID MAC Address = 0:23:124:47:182:154
[05/09/14 13:13:49.430 IST 64c1 211] AAA SRV(00000118): process author req
[05/09/14 13:13:49.430 IST 64c2 211] AAA SRV(00000118): **Author method=SERVER_GROUP**
Zubair_ISE
[05/09/14 13:13:49.430 IST 64c3 211] Parsed CLID MAC Address = 0:23:124:47:182:154
[05/09/14 13:13:49.430 IST 64c4 211] AAA SRV(00000000): process response req

[05/09/14 13:13:49.469 IST 64c5 220] **AAA SRV(00000118): protocol reply PASS for Authorization**
[05/09/14 13:13:49.469 IST 64c6 220] **AAA SRV(00000118): Return Authorization status=PASS**
[05/09/14 13:13:49.469 IST 64c7 8151] 0017.7c2f.b69a AAAS: received response, cid=268
[05/09/14 13:13:49.469 IST 64c8 8151] 0017.7c2f.b69a AAAS: deleting context, cid=268
[05/09/14 13:13:49.469 IST 64c9 8151] 0017.7c2f.b69a Not comparing because the ACLs have not been sent yet.
[05/09/14 13:13:49.469 IST 64ca 8151] 0017.7c2f.b69a Final flag values are, epmSendAcl 1, epmSendAclDone 0
[05/09/14 13:13:49.469 IST 64cb 8151] 0017.7c2f.b69a client incoming attribute size are 77
 --More--
[05/09/14 13:13:49.469 IST 64cc 8151] 0017.7c2f.b69a AAAS: mac filter callback status=0 uniqueId=280
[05/09/14 13:13:49.469 IST 64cd 8151] 0017.7c2f.b69a Local Policy: At the start of apfApplyOverride2. Client State RUN

[05/09/14 13:13:49.469 IST 64ce 8151] 0017.7c2f.b69a Applying new AAA override for station 0017.7c2f.b69a
[05/09/14 13:13:49.469 IST 64cf 8151] 0017.7c2f.b69a Local Policy: Applying new AAA override for station
[05/09/14 13:13:49.469 IST 64d0 8151] 0017.7c2f.b69a Override Values: source: 2, valid_bits: 0x0000, qosLevel: -1 dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout: -1
[05/09/14 13:13:49.469 IST 64d1 8151] 0017.7c2f.b69a dataAvgC: -1, rTAvgC: -1, dataBurstC: -1 rTimeBurstC: -1, vlanIfName: , aclName:
[05/09/14 13:13:49.469 IST 64d2 8151] 0017.7c2f.b69a Local Policy: Applying override policy
[05/09/14 13:13:49.469 IST 64d3 8151] 0017.7c2f.b69a Clearing Dhcp state for station ---
[05/09/14 13:13:49.469 IST 64d4 8151] 0017.7c2f.b69a Local Policy: Before Applying WLAN policy AccessVLAN = 12 and SessionTimeout is 1800 and apfMsTimeout is 1800

[05/09/14 13:13:49.469 IST 64d5 8151] 0017.7c2f.b69a Local Policy:Setting Interface name e VLAN0012

[05/09/14 13:13:49.469 IST 64d6 8151] 0017.7c2f.b69a Local Policy:Setting local bridging VLAN name VLAN0012 and VLAN ID 12

[05/09/14 13:13:49.469 IST 64d7 8151] 0017.7c2f.b69a Applying WLAN ACL policies to client
[05/09/14 13:13:49.469 IST 64d8 8151] 0017.7c2f.b69a No Interface ACL used for Wireless client in WCM(NGWC)
[05/09/14 13:13:49.469 IST 64d9 8151] 0017.7c2f.b69a apfApplyWlanPolicy: Retaining the ACL recieved in AAA attributes 255 on mobile
[05/09/14 13:13:49.469 IST 64da 8151] 0017.7c2f.b69a Local Policy: After Applying WLAN policy AccessVLAN = 12 and SessionTimeout is 1800 and apfMsTimeout is 1800

[05/09/14 13:13:49.469 IST 64db 8151] 0017.7c2f.b69a Local Policy: After Applying Site Override policy AccessVLAN = 12 and SessionTimeout is 1800 and apfMsTimeout is 1800

[05/09/14 13:13:49.469 IST 64dc 8151] 0017.7c2f.b69a Inserting AAA Override struct for mobile
   MAC: 0017.7c2f.b69a , source 2

[05/09/14 13:13:49.469 IST 64dd 8151] 0017.7c2f.b69a Inserting new RADIUS override into chain for station 0017.7c2f.b69a
[05/09/14 13:13:49.469 IST 64de 8151] 0017.7c2f.b69a Override Values: source: 2, valid_bits: 0x0000, qosLevel: -1 dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout: -1
[05/09/14 13:13:49.469 IST 64df 8151] 0017.7c2f.b69a dataAvgC: -1, rTAvgC: -1, dataBurstC: -1 rTimeBurstC: -1, vlanIfName: , aclName:
[05/09/14 13:13:49.469 IST 64e0 8151] 0017.7c2f.b69a Local Policy: After ovr check continuation
[05/09/14 13:13:49.469 IST 64e1 8151] 0017.7c2f.b69a Local Policy: apf_ms_radius_override.c apfMsSumOverride 447 Returning fail from apfMsSumOverride
[05/09/14 13:13:49.469 IST 64e2 8151] 0017.7c2f.b69a Local Policy: Calling applyLocalProfilingPolicyAction from Override2

[05/09/14 13:13:49.469 IST 64e3 8151] 0017.7c2f.b69a

```
**** Inside applyLocalProfilingPolicyAction ****

[05/09/14 13:13:49.469 IST 64e4 8151] 0017.7c2f.b69a *** Client State = RUN instance = 2
instance Name POLICY_PROFILING_L2_AUTH, OverrideEnable = 1 deviceTypeLen=0,
deviceType=(null), userRoleLen=0, userRole=(null)

[05/09/14 13:13:49.469 IST 64e5 8151] 0017.7c2f.b69a     Local Profiling Values :
isValidVlan = 0, vlan = 0, isVlanRecdInDelete = 0, isValidSessionTimeout = 0,
 sessionTimeout=0, isSessionTORecdInDelete = 0  ProtocolMap = 0 ,applyPolicyAtRun= 0
[05/09/14 13:13:49.469 IST 64e6 8151] 0017.7c2f.b69a          ipv4ACL = [],
ipv6ACL = [], inQoS = [unknown], outQoS = [unknown]
[05/09/14 13:13:49.469 IST 64e7 8151] 0017.7c2f.b69a Local Policy: At the End AccessVLAN
= 12 and SessionTimeout  is 1800 and apfMsTimeout is 1800

[05/09/14 13:13:49.469 IST 64e8 8151] 0017.7c2f.b69a In >= L2AUTH_COMPLETE for station
0017.7c2f.b69a
[05/09/14 13:13:49.469 IST 64e9 8151] 0017.7c2f.b69a AAAS: creating accounting interim
record using method list Zubair_ISE, passthroughMode 1
[05/09/14 13:13:49.469 IST 64ea 8151] 0017.7c2f.b69a AAAS: initialised accounting interim
request, uid=280 passthrough=1
[05/09/14 13:13:49.469 IST 64eb 8151] 0017.7c2f.b69a AAAS: accounting request sent
[05/09/14 13:13:49.469 IST 64ec 8151] 0017.7c2f.b69a Not Using WMM Compliance code qosCap 00
[05/09/14 13:13:49.469 IST 64ed 8151] 0017.7c2f.b69a In SPI call for >= L2AUTH_COMPLETE
for station  0017.7c2f.b69a
[05/09/14 13:13:49.469 IST 64ee 8151] 0017.7c2f.b69a WCDB_AUTH: Adding opt82 len 0
[05/09/14 13:13:49.469 IST 64ef 8151] 0017.7c2f.b69a WCDB_LLM: prev Mob state 3 curr Mob
State 3 llReq flag 0
[05/09/14 13:13:49.469 IST 64f0 8151] 0017.7c2f.b69a WCDB_CHANGE: auth=RUN(4) vlan 12
radio 0 client_id 0x47ad4000000145 mobility=ExpForeign(3) src_int 0x506c800000000f
dst_int 0x75e18000000143 ackflag 2 reassoc_client 0 llm_notif 0 ip  10.105.135.190
ip_learn_type DHCP
 --More--
[05/09/14 13:13:49.469 IST 64f1 8151] 0017.7c2f.b69a apfMsAssoStateInc
[05/09/14 13:13:49.469 IST 64f2 8151] 0017.7c2f.b69a apfPemAddUser2 (apf_policy.c:197)
Changing state for mobile  0017.7c2f.b69a  on AP  c8f9.f983.4260  from AAA Pending to
Associated

[05/09/14 13:13:49.469 IST 64f3 8151] 0017.7c2f.b69a Reason code 0, Preset 4, AAA cause 1
[05/09/14 13:13:49.469 IST 64f4 8151] 0017.7c2f.b69a Scheduling deletion of Mobile Station:
 (callerId: 49) in 1800 seconds
[05/09/14 13:13:49.469 IST 64f5 8151] 0017.7c2f.b69a Ms Timeout = 1800,
Session Timeout = 1800

[05/09/14 13:13:49.469 IST 64f6 207] [WCDB] ==Update event: client (0017.7c2f.b69a)
client id:(0x47ad4000000145) vlan (12->12) global_wlan (15->15) auth_state (RUN->RUN)
mob_st<truncated>
[05/09/14 13:13:49.469 IST 64f7 207] [WCDB] ===intf src/dst
(0x506c800000000f->0x506c800000000f)/(0x75e18000000143->0x75e18000000143) radio/bssid
(0->0)/(c8f9.f983.4260->c8f9.f983.4260) llm_notify (false) addr v4/v6 (<truncated>
[05/09/14 13:13:49.469 IST 64f8 207] [WCDB] wcdb_client_mcast_update_notify: No mcast
action reqd
[05/09/14 13:13:49.469 IST 64f9 207] [WCDB] wcdb_ffcp_wcdb_client_update_notify client
(0017.7c2f.b69a) id 0x47ad4000000145 ffcp update with flags=0x0
[05/09/14 13:15:47.411 IST 650a 8151] 0017.7c2f.b69a Acct-interim update sent for
station 0017.7c2f.b69a
[05/09/14 13:16:38.431 IST 650b 8151] 0017.7c2f.b69a
Client stats update: Time now in sec 1399621598, Last Acct Msg Sent at 1399621547 sec
```

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.